

Cyberviolence against Women and Girls in Zimbabwe: Prevalence, Nature, Impact and Strategies for Prevention

Ngonidzashe Zanamwe¹, Cross Gombiro², Taurai Rupere³, Viola J Jowa⁴, Plaxedes Mhlanga⁵, Edmore Mlambo⁶, Fungai N. Mukora⁷, Teurai Matekenya⁸, Munyaradzi Michael⁹

Abstract

This paper investigates cyberviolence against women and girls (WAG) in Zimbabwe, a context marked by growing internet access, weak legal enforcement, lack of digital rights awareness, significant digital gender gap and patriarchal social norms. Cyberviolence involves using digital technologies to harass, threaten, embarrass and target people. Three theoretical frameworks guided this research: the Technology-Facilitated Gender-Based Violence Framework, Routine Activity Theory, and Feminist Theory. Together, these frameworks informed research instrument design and the interpretation of findings. The research employed a mixed methods approach with 177 participants. Key findings indicate that 20% of WAG experienced cyberviolence, predominantly on Facebook, X and WhatsApp in the forms of cyberbullying (26.2%), cyberstalking (18.8%), and cyber harassment (15.0%). Among those affected, 80.6% encountered cyberviolence one to five times in the past year. While 91% viewed cyberviolence as a serious issue, 58.2% were unaware of the Cyber and Data Protection Act, and 33.8% deemed its protections inadequate. The main psychological impacts included anxiety (13.5%), depression (12.1%), and reputational harm (11.3%). Respondents took actions such as blocking perpetrators (26.1%), avoiding bullies (12.5%), confronting perpetrators (11.4%), and leaving the digital platforms (8.0%). Recommendations included awareness campaigns, stricter cyberviolence laws, anonymous reporting platforms, and improved training for law enforcement to adequately address cyberviolence.

Keywords: gender-based violence, cyberviolence, cyberbullying, women and girls, ICT-facilitated violence

1 Introduction

1.1 Background

Cyberviolence Against Women and Girls (CVAWG) is a growing aspect of gender-based violence (GREVIO, 2021). This form of violence is perpetrated through digital technologies and the Internet (Cybersafe, 2020), leading to serious consequences that manifest as sexual, physical, economic, or psychological harm to women and girls (WAG), as indicated by the European Institute for Gender Equality (2022). Sadly, WAGs frequently withdraw from the digital realm, leading to silencing and isolation, ultimately depriving them of opportunities for educational advancement, professional development, and establishing support networks (European Institute for Gender Equality, 2022). CVAWG encompasses threats such as coercion and arbitrary deprivation of liberty in both public and private spheres (World Health Organisation, 2020). Although individuals of all genders may experience cyberviolence, WAG are disproportionately subjected to repeated and severe forms of sexual, psychological, physical, or emotional abuse, often suffering significant consequences as a result (GREVIO, 2021; European Institute for Gender Equality, 2022). Consequently, this study aims to provide a comprehensive understanding of CVAWG in Zimbabwe.

¹ Computer Science Department, University of Zimbabwe, Harare, Zimbabwe, nzanamwe@ceic.uz.ac.zw

² Computer Science Department, University of Zimbabwe, Harare, Zimbabwe, cgombiro@ceic.uz.ac.zw

³ Computer Science Department, University of Zimbabwe, Harare, Zimbabwe, trupere@ceic.uz.ac.zw

⁴ Computer Science Department, University of Zimbabwe, Harare, Zimbabwe, vjowa@ceic.uz.ac.zw

⁵ Computer Science Department, University of Zimbabwe, Harare, Zimbabwe, pmhlanga@ceic.uz.ac.zw

⁶ Computer Science Department, University of Zimbabwe, Harare, Zimbabwe, emlambo@ceic.uz.ac.zw

⁷ Computer Science Department, University of Zimbabwe, Harare, Zimbabwe, fmukora@ceic.uz.ac.zw

⁸ Computer Science Department, University of Zimbabwe, Harare, Zimbabwe, tmatekenya@ceic.uz.ac.zw

⁹ Computer Science Department, University of Zimbabwe, Harare, Zimbabwe, mmunyaradzi@ceic.uz.ac.zw

1.2 Statement of the Problem

Cyberviolence against WAG is a growing concern, particularly in low and middle-income countries, where the rise of digital technologies has created new avenues for abuse. The situation is further worsened in Zimbabwe by weak legal enforcement, lack of digital rights awareness, significant digital gender gap and patriarchal social norms. Cyberviolence has been widely investigated in literature, and up to 85% of women globally have encountered some form of online violence. However, the existing literature lacks comprehensive data on the specific experiences of WAG in Zimbabwe, leading to significant underreporting and inadequate policy responses. This research investigates the prevalence, nature and impact of cyberviolence against WAG in Zimbabwe, aiming to fill the knowledge gap. Such an investigation is essential not only for reducing the incidence of cyberviolence but also for providing policymakers with actionable recommendations and a critical foundation for understanding the unique challenges faced by WAG in the context of technological advancements. Ultimately, the findings of this study will contribute to efforts by organisations, individuals, and the nation to create a safer cyberspace for all users.

1.3 Aim and Objectives

This study aimed to investigate cyberviolence among Zimbabwean WAG with the objectives of determining (i) the prevalence of online and cyberviolence against women and girls (CVAWG), (ii) the nature of CVAWG, (iii) the impact of CVAWG and (iv) strategies for prevention of CVAWG.

2 Related Work

This study draws on a wider range of both local and global scholarship. For instance, Moffat (2024) provides an important Zimbabwean perspective through an examination of cyberbullying among Zimbabwean female social media influencers, highlighting the online risks faced by women in public digital spaces and the gaps in local enforcement mechanisms. This complements Chiome's (2015) work on gender and ICTs in Southern Africa, which contextualises how unequal access and cultural norms exacerbate risks for WAG in digital spaces. At the global level, Noble's (2018) influential work on algorithmic oppression demonstrates how bias embedded in digital technologies can deepen vulnerabilities, while Dunn (2020) expands the discussion by identifying emerging forms of online harassment that go beyond traditional cyberbullying. Additionally, Lewis et al. (2019) emphasise feminist approaches to online gender violence, arguing for intersectional frameworks that capture the layered nature of harm. This builds on the typologies of cyberbullying proposed by Kowalski et al. (2014), which remain foundational in understanding the different modalities of digital abuse.

To improve conceptual clarity, this study distinguishes between legal and socio-psychological definitions of cyberviolence. Legally, Zimbabwe's Cyber and Data Protection Act (2021) criminalises cyberbullying, harassment, and the non-consensual sharing of intimate images, offering a statutory baseline. Socio-psychological definitions, however, as highlighted in global literature, emphasise the emotional, reputational, and relational harm experienced by victims (Kowalski et al., 2014; Lewis et al., 2019). This two-part framework ensures that cyberviolence is examined both as a legal violation and as a deeply social and psychological phenomenon, enriching the analysis of its impact on WAG.

2.1 Forms of Cyberviolence Against Women and Girls

Cyberviolence encompasses various harmful behaviours facilitated by digital technologies, such as social media platforms, the Internet, and instant messaging. Common forms of cyberviolence include **cyberbullying**, **cyber harassment**, **cyberstalking**, **non-consensual intimate image abuse**, and **online gender-based hate speech**, along with less common behaviours like **impersonation**, **online threats**,

doxing, identity theft, trolling, flaming, and body shaming (European Institute for Gender Equality, 2022; Hinson, Mueller, O'Brien-Milne and Wandera, 2018).

Cyberbullying is a common form of cyberviolence which refers to the deliberate and repeated unlawful and intentional use of ICTs (Internet, phone, computer, email, WhatsApp, Facebook, X, etc.) to intimidate, coerce, harass, bully, threaten or cause substantial emotional distress, or to humiliate, degrade or demean the person of another or to encourage a person to harm himself or herself (Zimbabwe Data Protection Act [Chapter 11:12], 2021; Hinduja and Patchin, 2015; Hinduja and Patchin, 2006; Saleem, Khan, and Zafar, 2021; Tokunaga, 2010 and Lee et al., 2017). Although there are several definitions of cyberbullying, common among them is that cyberbullying is a *deliberate* and, most importantly, *repeated* act in which some harm is done to an individual or group using digital technologies. Forms of cyberbullying include excluding people from digital groups, spreading rumours digitally, sending nasty texts, chats or comments and impersonating someone (OECD, 2017).

Cyber harassment involves the use of digital technologies to intentionally humiliate, offend, annoy, threaten, alarm, attack, or insult a victim (Maras, 2016), and one incident is sufficient, although it may also involve more than a single incident (UNODC, 2019). On the other hand, cyberstalking is an array of threatening behaviours (UNODC, 2019), is methodical and persistent and involves repeated incidents (European Institute for Gender Equality, 2022). Cyber harassment can manifest in various forms and often intersects with other types of online violence (EIGE, 2017; APC, 2017, UNODC, 2019). It may involve sending unwanted and threatening messages through email, text, or social media platforms. Additionally, it can include inappropriate or offensive remarks in social networks or chat rooms, as well as online verbal abuse and threats of physical harm or death. Other forms include hate speech, the theft or dissemination of personal information, images, and videos, and the spreading of false information or rumours aimed at damaging a person's reputation.

2.2 Prevalence of Cyberviolence Against Women and Girls

The prevalence of cyberbullying and perpetration is very heterogeneous because of differences in study methodologies used to measure prevalence (Gottschalk, 2022). In a study conducted in 2020 in Zimbabwe, it emerged that cyberbullying was very high, with 75% of participants having received a threatening message, while 83% saw offensive messages while socialising online (Sibanda, 2020). In a study that analysed the treatment of female politicians in Zimbabwe through an examination of posts on X, it was established that social media was used to harass them and had to contend with diverse forms of sexist harassment online (Ncube and Gwatisira, 2020). In another study, which explored the extent and forms of cyber-bullying in Zimbabwean schools, it was found that 89% of high school teenage female students reported some form of cyberbullying (Chiome, 2014). These seemingly high figures are a cause for concern.

While Zimbabwean data remain limited, regional studies highlight comparable and sometimes higher levels of exposure to online gender-based violence. Table 2-1 summarises prevalence rates across selected countries, providing a comparative backdrop for Zimbabwe.

Table 2-1: Regional Prevalence of Cyberviolence Against Women and Girls

Country	Study/Year	Prevalence (%)	Research centred on
Zimbabwe	Sibanda (2020)	75%	Higher in schools and universities
Malawi	Malanga (2021)	83–92%	Cyberbullying and harassment are dominant
South Africa	Mabika and Dube (2017)	58.5%	University students
Nigeria	Olasanmi et al. (2020)	53.9%	Students sample

Egypt	Hassan et al. (2020)	41.6%	National female survey
Pakistan	Saleem et al. (2021)	90%	University students

2.3 Impact of Cyberviolence Against Women and Girls

Cyberbullying as a form of cyberviolence can have serious consequences for the WAG, including negative impacts on self-esteem and self-worth (Kowalski et al., 2014), feelings of loneliness and social isolation leading to mental health problems (Bonanno and Hymel, 2013), stress-related health problems such as gastrointestinal problems and headaches (Beran and Li, 2005), negatively impact the victims' social relationships (Landoll et al., 2015; Navarro et al., 2019), decreased academic performance and job productivity (Wang et al., 2018), job dissatisfaction and hindering with career advancement opportunities (Einarsen and Nielsen, 2015), permanent emotional trauma and post-traumatic stress disorder (Smoktunowicz et al., 2020), high levels of anxiety and depression (Hinduja and Patchin, 2010). The verbal online violence and harassment against female politicians set out to call them to submission to the patriarchal gatekeepers of political power (Ncube and Gwatisira, 2020).

2.4 Strategies for Prevention of Cyberviolence Against Women and Girls

One effective strategy for preventing cyberviolence against WAG involves comprehensive educational campaigns and empathy training, coupled with robust legal frameworks (Willard, 2011; Ang and Goh, 2010; Olanmi et al., 2020; Poulpunitha et al., 2020; European Institute for Gender Equality, 2022). While Zimbabwe has established the Cyber and Data Protection Act (2021) and a POTRAZ Cybersecurity Centre, its approach is critiqued for being overly punitive, lacking victim support, and suffering from weak enforcement due to insufficient training (Al-Nasrawi, 2021; Moffat, 2024). Recent studies underscore the urgency of this issue and suggest a needed shift towards more preventive, community-driven awareness campaigns and survivor-centred frameworks, as seen in other regional contexts (Sheikh and Rogers, 2024; Malanga, 2021; Mabika and Dube, 2017).

Based on the literature, critical research gaps on CVAWG in Zimbabwe include a lack of comprehensive national data and a pronounced urban bias in existing studies, limiting understanding of rural experiences. Open questions include, what is the prevalence of CVGWG in Zimbabwe? What are the predominant forms of cyberviolence? How does cyberviolence affect WAG? And what strategies can effectively prevent and address cyberviolence?

2.5 Theoretical Frameworks

This study draws upon three complementary theoretical perspectives to analyse CVAWG in Zimbabwe, situating the phenomenon within both digital and socio-structural contexts. The first is the Technology-Facilitated Gender-Based Violence (TFGBV) Framework (Hinson, Mueller, O'Brien-Milne and Wandera, 2018). The framework examines the motivations and intentions of perpetrators, the specific behaviours and strategies they employ—such as the mode and frequency of abuse—and the resulting impacts on survivors, which vary according to the relationship between victim and perpetrator. Critically, it also addresses survivors' help-seeking and coping mechanisms, thereby providing a holistic view of the abuse cycle from initiation to response. However, its primary weakness is its limited emphasis on the broader socio-political and legal contexts that shape both perpetration and victimisation.

A second crucial lens is provided by Routine Activity Theory (RAT) (Cohen and Felson, 1979), which posits that crime occurs when three elements converge in time and space: a motivated offender, a suitable target, and the absence of a capable guardian. In the context of cyber violence, WAGs who are active online become suitable targets due to their visibility and accessibility, a reality reflected in recent studies showing high rates of social media usage among young Zimbabwean women paired with low digital safety awareness (Mhlanga, 2022). Perpetrators, often shielded by anonymity, act as motivated offenders

exploiting digital environments where guardianship—whether in the form of effective platform moderation, robust cybersecurity measures, or enforceable legal frameworks—is frequently weak or absent, as noted in critiques of the enforcement gaps within Zimbabwe’s Cyber and Data Protection Act (Moyo and Sibanda, 2023; Henson et al., 2013). Nevertheless, a key limitation of RAT is its under-theorisation of the offender's motivations, particularly the gendered and ideological drivers central to cyber violence against women.

The third and foundational perspective is Feminist Theory, which roots online harassment within systemic patriarchal power structures and gender inequality. Feminist theory frames online harassment as an extension of systemic gender inequality, where digital platforms reinforce patriarchal control to silence women and uphold gender norms (Citron, 2014; Hooks, 2000; Jane, 2020). It emphasises intersectionality, where women with marginalised identities—such as women of colour, disabled women, or those in rural areas—experience compounded and more severe forms of abuse due to layered social and structural inequities (Noble, 2018; Machiri and Maphosa, 2024). This pattern is evident in Zimbabwe, where female politicians and activists are disproportionately targeted (Chibuwe and Ureke, 2021), a reality exacerbated by infrastructural gaps and entrenched social stigma. The principal weakness of the theoretical framework is that it can sometimes lack specific, actionable mechanisms for explaining the immediate situational opportunities that offenders exploit in digital spaces.

A hybrid conceptual framework was developed (Figure 2-1) drawing from the three theoretical frameworks and this new conceptual framework offers a multi-layered analysis in that the Feminist Theory reveals the structural and ideological roots of gendered abuse; RAT clarifies the situational and opportunistic conditions that facilitate it; and the TFGBV framework details the specific behaviours, impacts, and coping responses associated with technology-facilitated harm. This integrated lens captures both the macro-level social dynamics and the micro-level behavioural mechanisms of cyber violence. It is grounded firmly in the Zimbabwean context, incorporating key legal instruments such as the Cyber and Data Protection Act (2021), the Domestic Violence Act, and Section 80 of the Constitution, alongside institutional actors like the Zimbabwe Republic Police (ZRP) and the Postal and Telecommunications Regulatory Authority (POTRAZ). Cultural dimensions—including the interplay between customary and statutory law, practices such as lobola, and barriers like social stigma, economic vulnerability, and underreporting—are also woven into this contextual understanding.

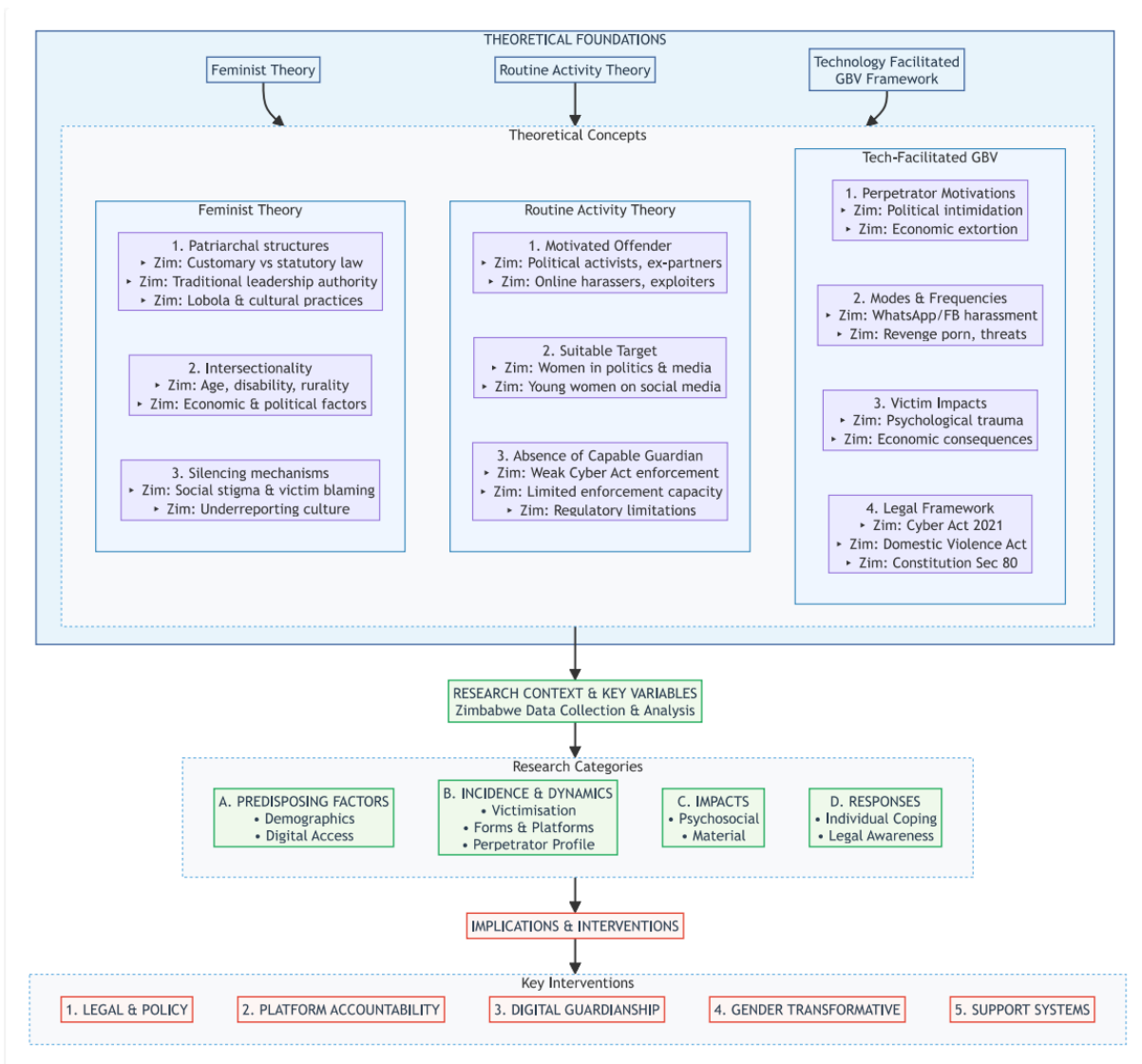


Figure 2-1: Conceptual Framework for Study of Cyber Violence Against Women and Girls in Zimbabwe

The above proposed conceptual framework aligns with specific study objectives: the TFGBV framework highlights the forms and modalities of abuse, informing analysis of its nature; RAT explains how online visibility and weak guardianship create conditions for victimisation, addressing prevalence and prevention; and Feminist Theory underscores the patriarchal power structures that underpin and amplify this abuse, connecting to impacts such as the silencing of women in public life. This theoretical triangulation ensures the study's aims are grounded in robust, practical explanatory models.

3 Methodology

A parallel mixed-methods research design was adopted for the study. This research design combined qualitative and quantitative research methods. This integrative approach allows researchers to draw on the strengths of both qualitative and quantitative data, providing a more comprehensive understanding of research problems than either method alone. Under the quantitative technique, the survey research method was used, whereas focus group discussions, key informant interviews and content analysis were used as qualitative research methods.

3.1 Constructs and Operationalised Variables

The conceptual framework for this study is built upon the understanding that CVAWG is a multifaceted issue influenced by legal, social, and technological factors, necessitating a dual operationalisation approach to bridge the gap between the legal definitions in Zimbabwe's Cyber and Data Protection Act (2021) and victims' nuanced subjective experiences. The prevalence was measured quantitatively by surveying experiences with specific abuses like non-consensual image sharing and doxing, while the nature and impact were assessed through a mixed-methods approach combining quantitative surveys on mental health and professional standing with qualitative interviews on lived experiences. Finally, constructs for prevention and response strategies were operationalised to assess awareness of legal rights and the key barriers to reporting, such as fear of re-victimisation and perceived apathetic responses from authorities, as established in the literature (Tourangeau and Yan, 2007).

3.2 Population and Sample Size Determination

The population comprised all Zimbabwean women and girls above 18 years. Given the large population size, surveying every individual was neither feasible nor cost-effective; therefore, a sampling method was used. The estimation formula for the sample size is given by,

$$n = \left(\frac{fz^2\hat{P}(1 - \hat{P})}{e^2 + \frac{z^2\hat{P}(1 - \hat{P})}{N}} \right) / r$$

where

- **n** is the parameter to be calculated and is the sample size in terms of the number of households to be selected;
- **z²** is the statistic that defines the level of confidence desired and the recommended is 95% which gives a z value of 1.96.
- **$\hat{P}$** is an estimate of a key indicator to be measured by the survey and 89% was used based on the 2022 National Housing Census
- **r** is a multiplier to account for the anticipated rate of non-response. The recommended one is an **r**-value lying between 0.8 and 1. An 80% response rate was used because this is an online survey.
- **e** is the margin of error to be attained and the recommended is 5%.
- **f** is the sample design effect. The recommended design effect is between 1 and 2. Using a design effect of 1.2 and incorporating the ten provinces, the resulting design effect is $f=1.2*10=12$.
- **N** is the population size of females who are at least 18 years. Based on the 2022 National Housing Census, there were 4,329,041 (ZIMSTAT, 2022 pp 111) females in Zimbabwe.

The resulting sample size was 188, which is shown in Table 3-1.

Table 3-1: Females Sample Size

Z	Z²	P	e	Design effect	Response rate	N	Domains	Sample
1.96(95%)	3.8416	0.89	0.05	1	0.80	4,329,041	1	188

A sample size of 188 was deemed representative and determined by a pragmatic approach, acknowledging the challenges of surveying sensitive topics as noted by Fincham (2008) and Dillman et al. (2014), where victims may be reluctant to disclose experiences due to fear of judgment, re-victimization, or lack of anonymity (Tourangeau and Yan, 2007; Hinduja and Patchin, 2014; Marwick and Boyd, 2014). This sample is comparable to the Economist Intelligence Unit's (2021) global report, which used fewer than 100 responses per country, and was distributed across Zimbabwe's 10 provinces proportionate to the population of females aged 18 and older, which totals 4,329,041 (ZIMSTAT, 2022, p. 111), making it robust for generating meaningful, policy-relevant insights.

3.3 Sampling Method

For the quantitative component, a convenience sampling strategy was employed. Researchers identified online women's groups with extensive female memberships, announced the study, and distributed a questionnaire link, which remained active for three months. This approach aligns with the methodology of Hassan et al. (2020). The qualitative phase utilised purposive sampling to select expert key informants, such as social workers and NGO leaders. Community-based women's organisations assisted in recruiting diverse focus group participants through a combined purposive and snowball sampling method.

3.4 Data Collection Methods

Data were collected through key informant interviews, focus group discussions (with 8–12 participants in 5 provinces), and a quantitative online survey disseminated via social media, email, and women's organisations; though no pilot was conducted due to resource constraints, instruments were adapted from validated tools and refined through expert review to ensure reliability (Van Teijlingen and Hundley, 2001; Hassan, 2006).

3.5 Data Analysis

Quantitative data were analysed using SPSS (Statistical Package for the Social Sciences) version 29 and Excel. During the data cleaning process, checks were performed to identify outliers and unusual results. Following this, descriptive and inferential analysis was conducted, resulting in the creation of tables and graphs that facilitated the interpretation of the data. Qualitative data were imported into ATLAS.ti 24 and coded. The *AI Code Suggest* tool provided initial support for theme generation. Relationships were then explored using the *Code Co-Occurrence* tool, while patterns were visualised with *Code-Document Analysis*.

4 Results and Discussion

4.1 Reliability of the data collection Instrument

Results in Table 4-1 reveal that the overall reliability (0.79) of the data collection instrument was acceptable. Different types of reliability coefficients were used, namely, Cohen's Kappa (κ), Cronbach's Alpha (α), and Kuder-Richardson 20 (KR-20), to measure the reliability of different sections within the instrument. All scores were above the minimum threshold of 0.7 (Bujang, Omar and Baharum, 2018), implying that the instrument used was reliable.

Table 4-1: Reliability of Data Collection Instrument

Section	N Items	Reliability Coefficient (Type)	Coefficient Range	Overall Reliability Score	Interpretation
Demographics	8	Cohen's Kappa (κ)	0.85–0.95	0.92	Excellent
Awareness Scale	7	Cronbach's Alpha (α)	0.68–0.71	0.70	Acceptable
Impact Scale	20	Cronbach's Alpha (α)	0.82–0.84	0.83	Good
Response Scale	21	Kuder-Richardson 20 (KR-20)	0.75	0.75	Acceptable
Open-ended Coding	5	Cohen's Kappa (κ)	0.72–0.76	0.74	Acceptable
Overall Instrument	61+	Composite Reliability (CR)	0.79	0.79	Acceptable

4.2 Response rate

The overall response rate was 94% (Table 4-2) and was high enough to eliminate non-response bias because response rates of 60% for most studies are ideal (Fincham, 2008). Other scholars (Babbie, 1990; Dillman, 2000) suggest 50% as the minimal response rate. This implies that population inferences can be made using sample results from this study.

Table 4-2: Response rates

Province	Target sample size	Actual sample size	Response rate
Bulawayo	17	17	100
Manicaland	29	29	100
Mashonaland Central	17	17	100
Mashonaland East	21	19	90
Mashonaland West	20	16	80
Matabeleland North	16	16	100
Matabeleland South	19	19	100
Midlands	12	12	100
Masvingo	13	13	100
Harare	24	19	79
Total	188	177	94

At the provincial level, the results in Table 4-2 above also show that each province has been represented adequately to eliminate non-response bias. This implies that sample results can be used to make population inferences. In addition, Harare province had the lowest response rate of 79%, while the highest response rate was 100%, which was recorded in seven provinces, as shown in Table 4-2.

4.3 Demographics

Only WAGs above the legal age of majority (18 years) in Zimbabwe across all ten provinces participated in the survey. Table 4-3 demonstrates that all age groups participated in the survey; therefore, the sample was representative of the population. Furthermore, 80.8% of the respondents were in the 18-35 years age group. This age group comprises active youths in using ICTs. In addition, only 1.1% of the respondents were over 60 years, while 18.1% were between 36 and 60 years.

Table 4-3: Distribution of respondents by age group

		Frequency	Percent	Valid%	Cumulative%
Valid	18- 35 years	143	80.8	80.8	80.8
	36 - 60 years	32	18.1	18.1	98.9
	Over 60 years	2	1.1	1.1	100.0
	Total	177	100.0	100.0	

Regarding disability status, survey results reveal that people with and without disabilities participated in the survey. Only 5.6% of the participants were living with disabilities, while the remaining 94.4% were living with no disabilities (Table 4-4). These statistics demonstrate that the sample was representative of the population; hence, sample results can be generalised to the entire population.

Table 4-4: Distribution of respondents by disability status

		Frequency	Percent	Valid%	Cumulative%
Valid	Disabled	10	5.6	5.6	5.6
	Not disabled	167	94.4	94.4	100.0
	Total	177	100.0	100.0	

Table 4-5 reveals that respondents were from both rural (5.1%) and urban areas (94.9%). This is because most urban respondents have easy access to the Internet, which was used in conducting the study. This can also be explained by the fact that most of these respondents are working (Table 4-7), probably in urban areas, as most had first degrees (Table 4-6).

Table 4-5: Distribution of Respondents by Community Setup

		Frequency	Percent	Valid%	Cumulative%
Valid	Rural	9	5.1	5.1	5.1
	Urban	167	94.4	94.9	100.0
	Total	176	99.4	100.0	
Missing	System	1	.6		
Total		177	100.0		

Study respondents came from diverse academic backgrounds (Table 4-6), with the highest proportion (54.8%) having a first degree, followed by those with higher degrees (20.3%) and 'A Level' certificates (13.1%).

Table 4-6: Distribution of respondents by highest educational qualification

		Frequency	Percent	Valid%	Cumulative%
Valid	O Level	2	1.1	1.1	1.1
	A Level	23	13.0	13.1	14.2
	Certificate	7	4.0	4.0	18.2
	Diploma	10	5.6	5.7	23.9
	First Degree	97	54.8	55.1	79.0
	Higher Degree	36	20.3	20.5	99.4
	Other Specify	1	.6	.6	100.0
	Total	176	99.4	100.0	
Missing	System	1	.6		
Total		177	100.0		

Regarding employment status, Table 4-7 reveals that respondents with different employment statuses participated in the survey. This indicates that the sample was a true reflection of the population. The highest percentage of respondents was formally employed (52.5%), while the lowest was self-employed (6.2%).

Table 4-7: Distribution of respondents by employment status

Province	Employment status			
	Not employed	Self-employed	Formally employed	Student
Bulawayo	23.50%	5.90%	52.90%	17.60%
Harare	6.90%	3.40%	72.40%	17.20%
Masvingo	5.90%	5.90%	58.80%	29.40%
Manicaland	21.10%	5.30%	42.10%	31.60%
Mashonaland Central	25.00%	6.20%	31.20%	37.50%
Mashonaland East	31.20%	0%	37.50%	31.20%
Mashonaland West	21.10%	5.30%	57.90%	15.80%
Matabeleland North	16.70%	0%	83.30%	0%
Matabeleland South	23.10%	7.70%	46.20%	23.10%
Midlands	31.60%	21.10%	36.80%	10.50%
Total	19.80%	6.20%	52.50%	21.50%

Study findings in Table 4-8 show that WAG had access to different digital platforms and the majority (31.8% + 29.6% + 28.1% = **89.5%**) had access to the Internet (Table 4-8) through the platforms (a smart mobile phone with internet access and camera, a social networking account and a laptop/desktop computer with internet access) they used. The fact that WAG had access to digital platforms exposed them to various forms of cyberviolence. This is further supported by other studies indicating that increased Internet access has become a breeding ground for various exclusionary and violent discourses and beliefs, which are often expressed and disseminated in an environment of anonymity and impunity (European Institute for Gender Equality, 2022).

Table 4-8: Digital platforms accessed by respondents

Digital platforms accessed	Percent
A 'smart' mobile phone (with internet access and camera)	31.8%
A social networking account (e.g. WhatsApp / Facebook / X, etc)	29.6%
A laptop/desktop computer (with internet access)	28.1%
A laptop/desktop computer (without internet access)	4.0%
An iPad (or other tablet) computer	3.8%
A mobile phone (without internet access)	2.7%
Total	100.0%

In terms of hours spent in a typical day by respondents using a mobile phone or computer or both, study findings in Figure 4-1 show that most of the respondents spent at least six (6) hours a day using a mobile phone or computer or both. Spending more time on digital platforms increased the exposure of WAG to cyberviolence.

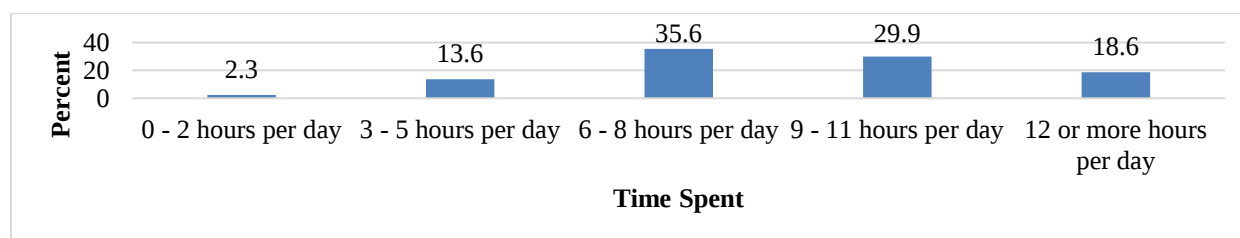


Figure 4-1: Hours in a typical day spent using a mobile phone or computer or both

4.4 Prevalence of cyberviolence

Figure 4-2 shows that 20% of the surveyed respondents were victims of cyberviolence, while the remaining 80% have never been subjected to cyberviolence. From a qualitative perspective, one of the respondents said, “Statistics show that 5-10 people are experiencing cyberbullying every day, there is bound to be bias in the statistics, which makes the risk even more daily”.

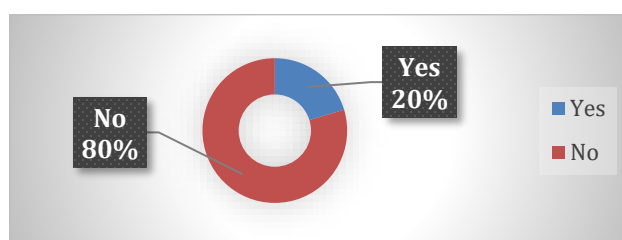


Figure 4-2: Have been a victim of cyberviolence

A *Logistic Regression Analysis* was conducted to identify predictors of cyber violence. The model incorporated the following variables: age (categorised as 18–35 versus 36 years and above), education level, and area of residence (rural versus urban). Key findings indicate that age is a significant predictor (odds ratio [OR] = 3.20; $p = .004$; 95% CI = 1.46–7.02). Women aged 18–35 were 3.2 times more likely to experience cyber violence than those aged 36 and above. Education level also emerged as a significant factor ($p = 0.032$). Compared to holders of O-Level qualifications, individuals with a higher degree were at 3.34 times greater risk (OR = 3.34; $p = 0.013$), while those with a first degree were at 2.44 times greater risk (OR = 2.44; $p = 0.034$). Finally, a significant geographic variation was observed. Women and girls residing in urban areas demonstrated a 2.1 times higher risk than their rural counterparts (OR = 2.10; $p = 0.045$).

Previous studies in Zimbabwe have shown that about 1.5% of the people in Zimbabwe encountered abuse of personal information and/or other privacy violations (ZIMSTAT, 2020). This seems to suggest that the prevalence of cyberviolence is increasing. Results of a study of Korean adolescents show that 14.6% of the respondents were victims of cyberbullying (Lee, 2017). This figure is lower than what was observed in this study and this variation is explained by Caridade, Braga, and Borrajo (2019) who argue that studies offer very different percentages of adolescents suffering cyber dating violence victimisation due to differences in the measurement instrument employed and the type of measured behaviours.

Victims of cyberviolence were asked to indicate how many times over the past twelve (12) months they experienced cyberviolence and the results are shown in Figure 4-3. These results suggest that 11.1% of the respondents experienced cyberviolence but not in the past twelve (12) months. The highest proportion (80.6%) of respondents in Figure 4-3 experienced cyberviolence between 1 and 5 times over the past twelve months. Interestingly, none of the respondents experienced cyberviolence between 6 and 10 times; however, 8.3% of the respondents experienced cyberviolence more than 11 times over the past twelve (12) months, which is quite worrying.

Three separate chi-square tests of independence were conducted. First, a significant association was found between victimisation status and awareness of the proposed Cyber and Data Protection Act ($\chi^2(1) = 8.34$, $p = 0.004$), with victims demonstrating greater awareness (82.4%) than non-victims (57.6%). Second, victimisation status was significantly associated with the type of online platform used ($\chi^2(3) = 15.72$, $p = 0.001$), with integrated social networking sites showing a significantly higher incidence of victimisation (74.5% of victims used these platforms). Third, the highest educational qualification was significantly associated with the reported frequency of experiencing cyber violence over the past 12 months ($\chi^2(12) = 21.45$, $p = 0.047$). Notably, 60.8% of those who reported being victims of cyber violence held a first degree as their highest qualification. These findings differ from findings in a study conducted in Egypt, where 45.3% of respondents reported multiple exposures to cyberviolence (Hassan et al., 2020), while in this Zimbabwean sample, only 37.3% (19/51) of victims reported multiple incidents.

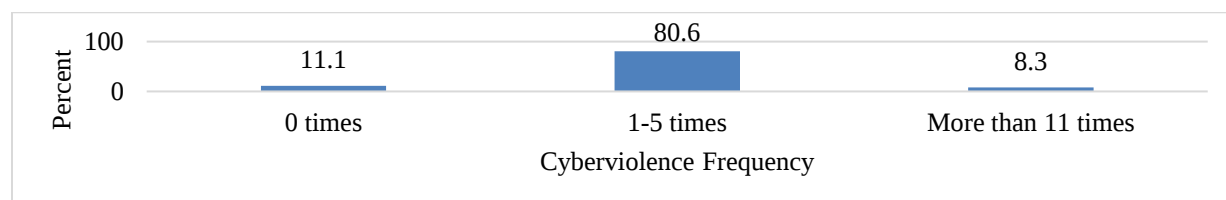


Figure 4-3: Frequency of cyberviolence in the previous 12 months

A *Logistic Regression Analysis* was further conducted to check if daily internet usage (in hours) was a predictor of cyber violence. Key findings indicate that daily internet usage was a significant predictor. For

every additional hour of use beyond six hours per day, the risk of cyber violence increased by a factor of 1.4 (OR = 1.40 per hour; $p = 0.009$; 95% CI = 1.1–1.8).

The practical implications of this analysis, derived from risk profile combinations, suggest that the highest risk of cyber violence is observed among young women (aged 18–35) who possess higher educational qualifications, engage in high levels of daily internet use, and reside in urban areas.

4.5 Awareness of the Cyber and Data Protection Act

Respondents were asked about their knowledge of the Cyber and Data Protection Act in Zimbabwe. The findings were that 41.8% (Table 4-9) of the respondents were aware of the Cyber and Data Protection Act. This figure is probably high because most of the surveyed respondents were literate and hence expected to know the Cyber and Data Protection Act. However, a rather high proportion (58.2%) of respondents said they were unaware of the Cyber and Data Protection Act. This is supported by one of the respondents who said, *“Firstly, the generality of women is not even aware of what cyber-violence is, so even when it is perpetrated, they are not aware. Also, even though I am aware, some attacks cannot be controlled or prevented, for example, a person luring you to eventually steal from you unless the victim is alert and reacts appropriately”*.

Table 4-9: Cyber and Data Protection Act Awareness

Response	Are you aware of the existence of the Cyber and Data Protection Act in Zimbabwe?	Are you aware that you are protected by the Cyber and Data Protection Act?
Yes	41.8%	85.1%
No	58.2%	14.9%

A Chi-square Test of independence reveals a significant relationship between the age of respondents and their awareness of the Cyber and Data Protection Act in Zimbabwe, χ^2 ($p = 0.006$). The analysis indicates that respondents aged 36–60 years demonstrated a higher level of awareness compared to other age cohorts. Furthermore, awareness was significantly associated with education level ($\chi^2(4)=11.83$, $p=0.019$), with postgraduates showing the highest awareness (94.1%), followed by first degree holders (86.7%), and lowest among those with O-Level qualifications (66.7%).

Of those respondents who are aware of the Cyber and Data Protection Act, the majority (85.1%) are aware that they are protected by it. The remaining 14.9% were unaware that the Cyber and Data Protection Act protects girls and women. One of the respondents, who was unaware, said, *“Very little information is readily available in the communities. Inasmuch as there is an Act, there should also be short pamphlets, fliers, billboards and even adverts on TV broadcasting this. Even socialites should come on board with skits making people aware of Cyberviolence, its effects and repercussions for the perpetrators”*.

With regards to whether the Cyber and Data Protection Act adequately protects women and girls against cyberviolence, 36.5% (Figure 4-4) of the surveyed respondents indicated that they did not know whether or not the Act adequately protects women and girls. The results also show that 33.8% of the respondents feel that the Cyber and Data Protection Act does not adequately protect women and girls against cyberviolence. However, 29.7% of the respondents think that the Cyber and Data Protection Act adequately protects women and girls against cyberviolence. An *Ordinal Logistic Regression* analysed perceptions of adequacy (Yes/I Don't Know/No), treating it as an ordinal outcome. The proportional odds assumption was met ($\chi^2=7.21$, $p=0.125$). Significant predictors included prior victimisation (OR=2.87, $p=0.008$), with victims being nearly three times more likely to perceive the Act as inadequate, and awareness of personal protection (OR=4.12, $p<0.001$), with those unaware being four times more likely to doubt adequacy.

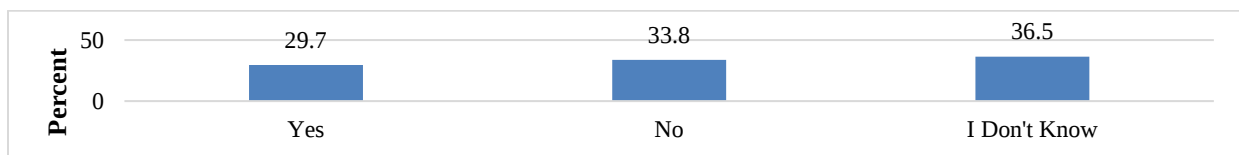


Figure 4-4: Cyber and Data Protection Act adequately protects women and girls against cyberviolence

4.6 Awareness of Cyberviolence

Respondents were asked to give their opinion on whether or not cyberviolence is a serious issue in Zimbabwe and the findings are in Figure 4-5. These results show that 91% of the surveyed respondents think that cyberviolence is a serious issue in Zimbabwe.

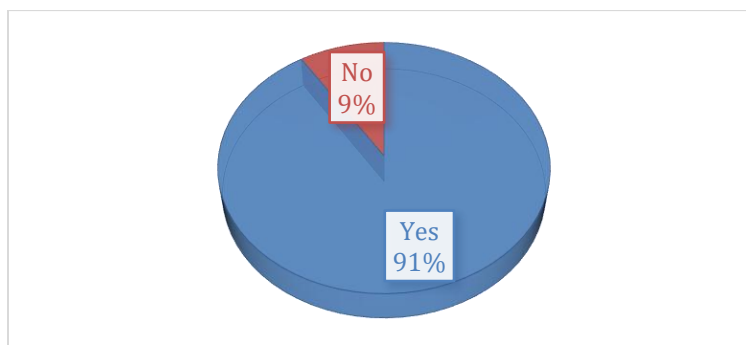


Figure 4-5: Cyberviolence is a serious issue in Zimbabwe

Further to agreeing that Cyberviolence is a major issue in Zimbabwe, most of the respondents (97.7%) indicated that more needs to be done to raise awareness of cyberviolence and its effects in Zimbabwe. This is supported by one respondent who said, *“not enough awareness and proof of consequences for perpetrators”*. Similar sentiments were echoed by another respondent who said, *“Most girls are unaware of the cyber protection”*. Logistic regression was conducted to examine demographic predictors of perceiving cyber violence as a serious issue (Yes=1, No=0). The model included age, education level, and employment status as predictors. Results revealed no statistically significant predictors (all p-values > 0.05).

Table 4-10: More needs to be done to raise awareness of Cyberviolence and its effects

		Frequency	Percent	Valid%	Cumulative%
Valid	Yes	172	97.2	97.7	97.7
	No	4	2.3	2.3	100.0
	Total	176	99.4	100.0	
Missing	System	1	.6		
Total		177	100.0		

Survey findings in Figure 4-6 show that the majority (58.3%) of perpetrators of cyberviolence were strangers, implying that they were not related to the victim. Despite a largely literate sample, the study found that 58.3% of women and girls were unaware of cyberviolence, and among those aware, 33.7% believed existing measures did not offer sufficient protection. *This highlights a gap between literacy and practical awareness, suggesting that formal education alone does not guarantee understanding of online risks or safety measures.* Factors such as inadequate information dissemination channels, limited outreach by government and civil society organizations, reliance on urban-centered communication strategies, and low engagement with social media or community forums where cyberviolence prevention messages might be shared could contribute to this lack of awareness. Additionally, awareness initiatives may not be tailored

to the everyday realities of women and girls, particularly in rural areas, further limiting comprehension and engagement. Recognizing these gaps is critical for designing more effective cyberviolence awareness campaigns, ensuring that both literate and semi-literate populations can access and understand protective strategies and reporting mechanisms.

Similarly, in a study done in Egypt, a huge percentage (92.6%) of the perpetrators were unknown (Hassan et al., 2020). This then makes it difficult to deal with this kind of violence against women and girls. Furthermore, the results revealed that 11.1% of the girls and women who engaged in cyberviolence were friends with the victims while 8.3% were either co-workers or relatives. Surprisingly, low proportions (2.8%) of girls and women indicated that work supervisors and teachers/lecturers perpetrated violence against them. The remaining 8.3% categorised as ‘other’ perpetrators included former spouses or exes and friends of friends.

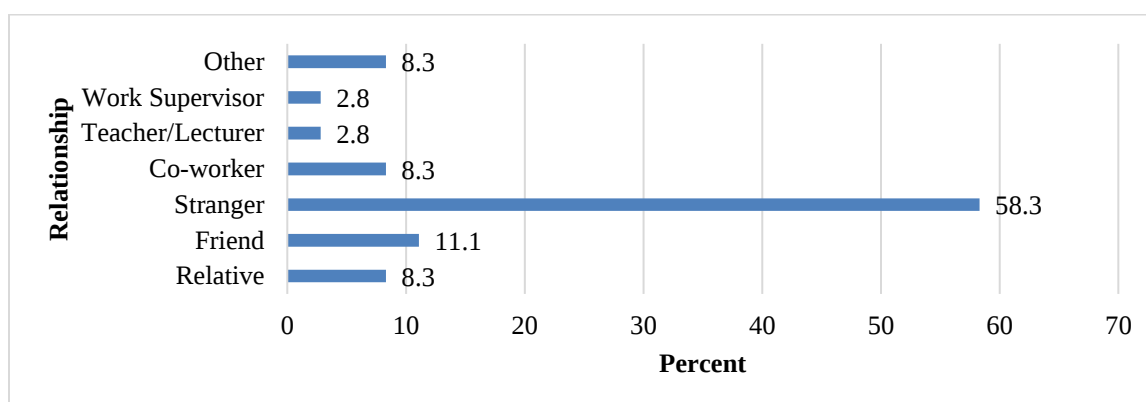


Figure 4-6: Relationship between the victim and perpetrator of cyberviolence

The study findings in Table 4-11 show that the majority (62.9%) of the perpetrators of cyberviolence were males, women accounted for 22.9% while the offender for the rest (14.2%) was not known.

Table 4-11: Cyberviolence perpetrator

Age of the perpetrator		Gender of the perpetrator		The perpetrator knew they committed Cyberviolence	
18-35 years	37.2%	Male	62.9%	Yes	20.0%
36 -60 years	31.4%	Female	22.9%	No	8.6%
Not Known	31.4%	Not Known	14.2%	Don't know	71.4%

Surprisingly, most perpetrators of cyberviolence (94%) did not take action to rectify the problem. This makes it difficult to address cyberviolence if the perpetrators are reluctant to rectify the problem. Gender disaggregation of results is key because it will inform strategies for the prevention of cyberviolence.

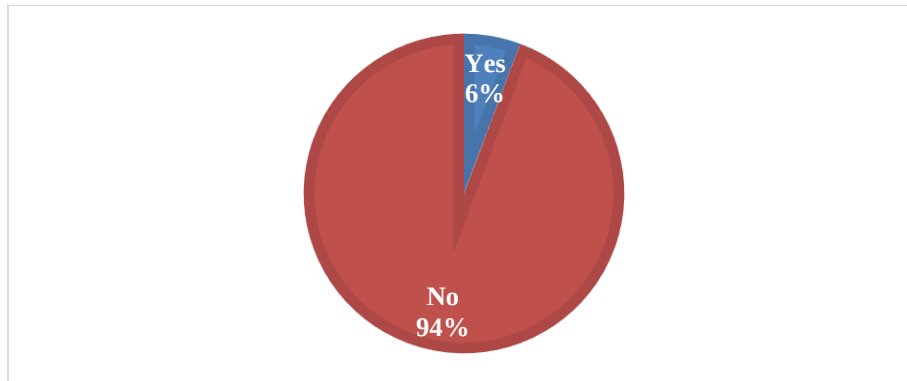


Figure 4-7: The perpetrator took action towards rectifying the problem

The highest proportion of perpetrators (31.4%) of cyberviolence were motivated by sexual desire (Figure 4-8) and this tallies with findings in the previous section that most of the perpetrators were male. A *Chi-square Test* found no significant association between perpetrator motive and relationship to the victim ($\chi^2(2)=2.641, p=0.267$). Despite the lack of statistical significance, Cramer's V (0.263) indicated a moderate practical effect, with a notable trend—strangers were more often motivated by sexual reasons, whereas known perpetrators tended to act out of jealousy or revenge.

The findings shown in Figure 4-8 to a lesser extent corroborate findings in a Malawian study in which it was established that motives for perpetrators were inspired by anger (76.4%), revenge (83.1%), political agenda (32.8%), sexual desire (59.7%) and jealousy (69.3%) (Malanga, 2021).

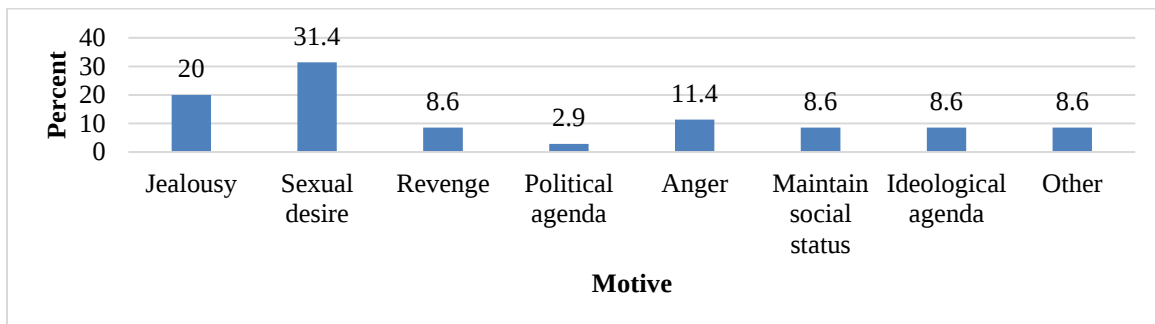


Figure 4-8: Motive for Committing Cyberviolence

Study findings in Figure 4-9 show that the majority of WAG (97%) in Zimbabwe felt that very little is being done to prevent cyberviolence. This finding means that the relevant authorities have a lot to do to curb cyberviolence. To support these findings, one of the respondents said, *“If that was the case, there would be many arrests made as it has become the norm”*. Another respondent was quoted saying, *“More awareness is needed so that the perpetrators are aware of cybercrimes and their consequences”*. Similar sentiments were shared by a respondent who said, *“Not enough awareness and proof of consequences for perpetrators”* and another one who said, *“Perpetrators are not brought to book”*. Lastly, another respondent echoed that, *“there was a need to employ applications that permit the user to first agree with all terms and conditions on a social media platform so that they are aware of the offence before, using all media platforms as means of awareness even to the hard-to-reach areas through radios and posters.”*

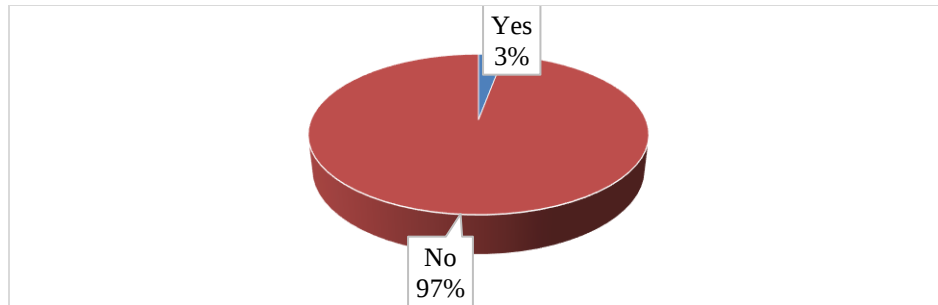


Figure 4-9: Is enough being done in Zimbabwe to prevent Cyberviolence?

Women and girls were asked whether they had knowledge about the procedures for reporting cyberviolence on online platforms such as WhatsApp, X, Facebook, Zoom, YouTube, etc. The results shown in Figure 4-10 reveal that 75% of the WAG did not know how to report cyberviolence on online platforms while only 25% were aware. As long as the majority of WAG are unaware of the reporting procedures for cyberviolence, combating it remains a pipeline dream.

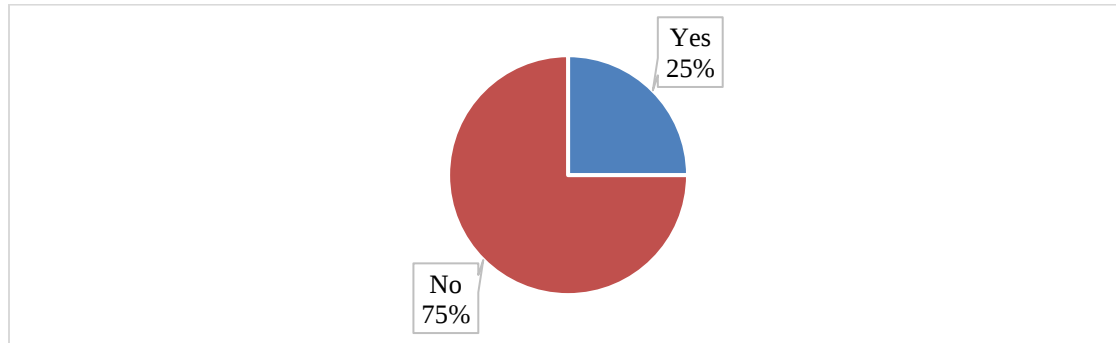


Figure 4-10: Knowledge of procedures for reporting cyberviolence on online platforms

4.7 Nature of online and ICT-facilitated VAWG

Regarding the nature of online and ICT-facilitated VAWG, Figure 4-11 shows that most women and girls were subjected to cyberbullying (26.2%), cyberstalking (18.8%), and cyber harassment (15.0%). A *Chi-square Test of Independence* revealed a significant association between the perpetrator's relationship to the victim and the type of cyber violence experienced ($\chi^2(4) = 12.45$, $p = .014$). Post-hoc analysis of adjusted residuals indicated that perpetrators who were strangers were disproportionately associated with cyberstalking, whereas known perpetrators, such as acquaintances or friends, were more frequently associated with cyberbullying.

A *factor analysis* using Principal Component Analysis of the cyber violence taxonomy revealed a three-factor structure, elucidating the underlying dimensions of online harm. The first extracted factor, accounting for 28.8% of the variance (Eigenvalue = 3.45), termed 'Intrusive Harassment', characterised by high loadings from cyber stalking (0.82) and cyber harassment (0.79). The second factor, explaining a further 17.7% of variance (Eigenvalue = 2.12), reflects 'Reputation Damage', defined primarily by online defamation (0.85) and online hate speech (0.72). A third distinct factor of 'Sexual Exploitation' emerged, accounting for 14.8% of variance (Eigenvalue = 1.78) and defined by online exploitation with sexual content (0.91) and non-consensual pornography (0.83). Collectively, this parsimonious model explains 61.3% of the total variance, indicating that these three constructs—Intrusive Harassment, Reputation Damage, and Sexual Exploitation—provide a robust empirical framework for conceptualising the primary typologies of cyber violence.

Consistent with the current findings, Hassan et al. (2020) identified that the most prevalent types of cyberviolence include cyberstalking and cyber harassment, which manifest as the receipt of symbols or images with sexual content, humiliating or offensive posts or comments, insulting messages or emails, violent or indecent images that demean women, and threats of sexual or physical violence. Additionally, the current findings align with those of Malanga (2021), who reported that cyberbullying (83.6%), cyberstalking (92.5%), online sexual exploitation (71.4%), and cyber harassment (76.1%) were the predominant forms of cyberviolence against women in Malawi.

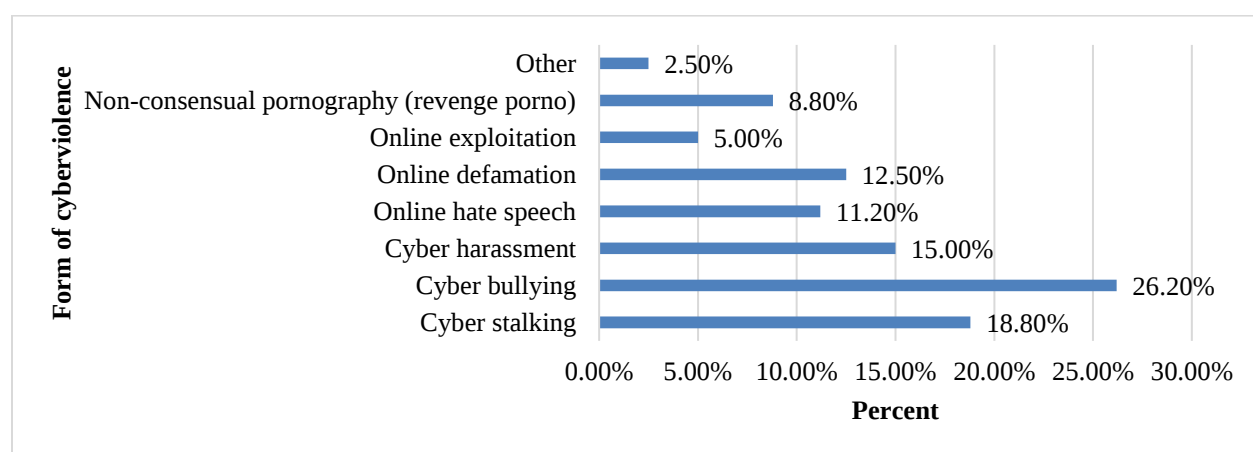


Figure 4-11: Form of cyberviolence experienced

4.8 Impact and strategies for prevention of online and ICT-facilitated VAWG

Online and ICT-facilitated VAWG impacted women and girls differently, as shown in Table 4-12. The top five impacts were anxiety (13.5%), depression (12.1%), harm to reputation or self-image damage (11.3%), cutting down from social activity (9.9%) and living in a state of fear (8.5%). The impacts classified as other in Table 4-12 include *distraction from the use of social media in an attempt to reinstall all social media applications, embarrassment, emotional stress, mood swings, loss of appetite to eat, repeatedly calling Human Resources until opting to resign and leave, loss of confidence and self-esteem for a long time, and feeling of vulnerability and lack of protection.*

Table 4-12: Cyberviolence impact

Category	Impact	Percent
Economic/Financial impact	Loss of income	2.1%
	Loss of educational opportunities	2.1%
	Inability to get a new job	2.1%
	Loss of home	1.4%
	Loss of property	1.4%
Physical impact	Physical illness	2.1%
	Physical abuse exacerbated by online violence	1.4%
	Physical harm and injury resulting from online violence	1.4%
Psychological/Emotional impact	Anxiety	13.5%
	Depression	12.1%
	Harm reputation/Self-image damaged	11.3%
	Living in a state of fear	8.5%
	Thoughts of suicide	5.0%
	Negative impact on job/school performance	5.0%

	Self-harming behaviours	2.8%
Social impact	Cut down on social activity	9.9%
	Isolated from family, friends or co-workers	7.8%
	Withdrew from online activity	5.7%
	Moved out of the community	1.4%
Other	Other	2.8%

To identify hidden and unobserved subgroups, a *Latent Class Analysis* (LCA) of the 21 dichotomous impact variables was conducted, and three distinct profiles of victim impact with robust model fit (BIC=1256.8, AIC=1012.3, entropy=0.88) were identified. The largest class, *Psycho-social Harm* (48.1%), was characterised by high probabilities of anxiety (0.92), depression (0.87), and living in fear (0.79). The *Reputational-Practical Harm* class (35.9%) showed high endorsement of reputation damage (0.94) and job/school performance impact (0.81). A smaller but severe *Multi-Systemic Harm* class (16.0%) exhibited high probabilities across psychological, social, practical, and physical domains, including self-harm ideation (0.68). A *Multinomial Logistic Regression* revealed the *Multi-Systemic* class was significantly associated with experiencing at least three forms of cyber violence (OR=4.3, $p<0.01$). Structural equation modelling confirmed a significant mediation pathway where *multiple victimisation forms* $\rightarrow$ *higher impact severity* $\rightarrow$ *greater likelihood of formal reporting* ($\beta=0.32$, $p<0.05$). These findings evidence that cyber violence impacts form distinct, clinically meaningful profiles directly influenced by victimisation complexity.

The results presented in Table 4-12 above are consistent with those found in similar studies, even though previous studies did not rank the findings according to popularity. Comparatively, Malanga (2021) established that cyberviolence is intended to physically (38.5%) and psychologically (61.8%) harm the victims or survivors. Similarly, Alotaibi and Mukred (2022) concluded that the serious consequences of cyberviolence include psychological harm, isolation, damage to a person's reputation, legal consequences and economic consequences.

In terms of courses of action taken after cyberviolence, study findings in Table 4-13 show that women and girls took several actions. Chief among them included, blocked attacker/perpetrator(s) on digital platforms (26.1%), avoided any further contact with the bully (12.5%), confronted attacker/perpetrator (s) (11.4%), left the digital/online platform(s) (8.0%), ignored all pictures or messages so that the bully loses interest (6.8%), never reported to police/community leaders (6.8%) and never sought intervention from owners of digital/online platforms (5.7%). It is disheartening to note that a relatively high proportion of WAG did not report incidences of cyberviolence either to the police or online platform owners. One of the reasons why WAG are not reporting is that no action is taken, as evidenced by an outcry from one of the respondents who said, "*People are being threatened by high-profile people not to report, that even if they report, nothing will be done to the perpetrator*". Another respondent weighed in by saying, "*Women are humiliated every day on Facebook and nothing happens. This cyberviolence cost me my job and marriage*". Another frustrated respondent mentioned one of the perpetrators and she said, "*xxxx keeps attacking women and nothing is being done at all*".

Table 4-13: Actions taken after cyberviolence

Action	Percent
Blocked attacker/perpetrator(s) on digital platforms	26.1%
Avoided any further contact with the bully	12.5%
Confronted attacker/perpetrator (s)	11.4%
Left the digital/online platform(s)	8.0%
Ignored all pictures/messages so that the bully loses interest	6.8%

Never reported to police/community leaders	6.8%
Never sought intervention from owners of the digital/online platforms	5.7%
Exposed the perpetrator/attacker (s) to their, friends, family and employers	4.5%
Left to a transition place/house/refuge	3.4%
Changed my contact details (phone number, email address, chat name, profile on social networking sites)	3.4%
Sought for health/social counselling services	2.3%
Wrote mean and threatening things to the bully	2.3%
Other	2.3%
Publicised perpetrator(s) personal information online	1.1%
Shared information with both online and print media	1.1%
Reported to the police and the attacker/perpetrator (s) was arrested	1.1%
Reported to the police but the police took no action	1.1%

A *Factor Analysis* of the 28 response actions extracted four distinct behavioural dimensions explaining 58.7% of variance— *Informal Coping* (blocking, ignoring), *Formal Reporting* (police, legal action), *Social Support Seeking* (counselling, telling family), and *Digital Self-Help* (changing contacts, platform appeals). A multivariate analysis of variance (MANOVA) found significant differences in factor scores by impact class (Wilks' $\Lambda=0.76$, $F=3.45$, $p<0.01$). Post-hoc tests revealed the *Multi-Systemic Harm* class scored significantly higher on *Formal Reporting* ($\eta^2=0.18$, $p<0.01$) and *Social Support Seeking* ($\eta^2=0.12$, $p=0.03$). A path analysis demonstrated a significant mediated relationship—*higher education* → *increased awareness of protection* → *greater Formal Reporting* (indirect $\beta=0.21$, $p=0.04$). However, a *Logistic Regression* showed *Formal Reporting* was not significantly associated with perpetrator apprehension ($OR=1.2$, $p=0.62$), indicating systemic enforcement gaps. These results reveal that victim responses are multidimensional, systematically related to impact severity, and constrained by both individual resources and institutional effectiveness.

The findings presented in Table 4-13 align with those of a study conducted in Egypt (Hassan et al., 2020), which identified blocking the perpetrator as the most prevalent response among victims. However, it is important to note that the percentages are not directly comparable; in the Egyptian study, a multiple-response format yielded 72%, whereas this study employed a single-response format, resulting in 26.1%. If the results from the Egyptian study are scaled down, 47% of females utilised blocking as a response, which remains higher than the figure obtained in this study. Furthermore, the results of the current study corroborate findings from research conducted in Malawi, where blocking perpetrators on digital platforms (50.7%), leaving the digital platform (26.9%), and confronting the perpetrator, either physically or digitally (10.4%), were identified as the most common responses to cyberviolence (Malanga, 2021).

4.9 Summary discussion

The findings of this study align with trends observed in both local and international contexts, highlighting the pervasive nature of cyberbullying. For instance, Khan, Shamsdin, Jabeen, and Asif (2025) reported similar patterns of online harassment and victimisation among social media users, emphasising the psychological and social impacts of cyberbullying across diverse populations. Locally, Mabika and Dube (2017) observed comparable experiences among Zimbabwean youths, noting that social media platforms often facilitate both the anonymity and reach that exacerbate cyberbullying behaviours. By situating the current results within these broader studies, the evidence underscores that the prevalence, forms, and consequences of cyberbullying are not confined to a single context but reflect a global phenomenon, while also highlighting context-specific factors relevant to Zimbabwe.

A feminist theoretical lens, however, is critical for understanding these patterns as manifestations of systemic patriarchal power rather than isolated technical malfeasance. The predominance of male

perpetrators (62.9%), the primary motivation of sexual desire (31.4%), and the severe psychological impacts (anxiety 13.5%, depression 12.1%) collectively demonstrate how cyberviolence functions as a tool for digital patriarchal control, silencing women and policing their participation in public online spaces. This structural perspective explains the significant enforcement gaps and underreporting identified, underscoring that effective solutions must address the underlying gender inequalities that fuel such abuse.

4.10 Generalizability and trustworthiness of findings

This study acknowledges several limitations that may affect the interpretation and generalizability of its findings. First, reliance on online-only data collection may introduce selection bias, excluding participants without internet access or with limited digital literacy. Second, the use of self-reported measures may be subject to response biases, including social desirability, recall bias, and underreporting of sensitive experiences such as cyberbullying (Tourangeau and Yan, 2007). Third, the relatively small sample size in certain regions may constrain the extent to which findings can be generalised across all demographic groups. Additionally, cultural and contextual factors unique to Zimbabwe may influence participants' willingness to disclose experiences, potentially affecting data accuracy (Marwick and Boyd, 2014; Hinduja and Patchin, 2014). Nonetheless, the mixed-methods design, integrating quantitative surveys with qualitative focus groups and content analysis, enhances the robustness of the results and supports cautious generalisation by triangulating multiple sources of data to provide a more comprehensive understanding of cyberbullying behaviours.

5 Conclusions and Recommendations

5.1 Conclusions

This study employed mixed methods to examine cyberviolence against women and girls in Zimbabwe, finding that 20% of the 177 surveyed participants were victims, primarily experiencing cyberbullying (26.2%), cyberstalking (18.8%), and harassment (15.0%). Key impacts included anxiety (13.5%) and depression (12.1%), while common responses were blocking perpetrators (26.1%) or avoiding contact (12.5%). A significant awareness gap was observed, with 58.2% unaware of the Cyber and Data Protection Act, and 91% believing cyberviolence is a serious issue requiring more awareness. The sample's urban bias (94.4%) limits rural generalizability but provides critical insights for policy, educational, and technological interventions, highlighting the need for future studies to include rural and younger demographics.

5.2 Recommendations

To address cyberviolence against women and girls in Zimbabwe, *short-, medium-, and long-term* recommendations with explicit stakeholder roles and monitoring mechanisms are suggested.

Short-term (0–12 months)

- Raise awareness of cyberviolence and digital rights. *Community-based workshops, social media campaigns, and engagement with influencers should target women and girls to close the law–awareness gap, particularly among urban and rural populations.*
- Introduce anonymous reporting platforms to encourage victims to report incidents without fear of retaliation. *Law enforcement agencies, NGOs, and mobile network operators should monitor usage statistics and user feedback to assess effectiveness.*
- Improve data collection by mandating annual national surveys and requiring law enforcement to publish statistics on cyberviolence. *This will provide baseline data for monitoring progress and evaluating interventions.*

Medium-term (1–3 years)

- Strengthen the Cyber and Data Protection Act and develop comprehensive cybercrime legislation. *This includes explicitly defining cyberviolence, ensuring stricter enforcement, and establishing specialized cybercrime courts. Parliament, Ministry of Justice, and police units should track enforcement outcomes and legal processes.*
- Establish a dedicated cybercrime unit within the police force, with officers trained to handle cyber-related gender-based violence cases sensitively and efficiently. *Unit performance should be monitored through case resolution rates and victim satisfaction surveys.*
- Integrate cyber safety education and digital literacy into school curricula, and make digital self-defence training widely available. *Ministry of Education, schools, and NGOs should assess knowledge gains and changes in online behaviour among participants.*

Long-term (3–5 years)

- Implement technological interventions, such as AI-powered content moderation tools, stronger default privacy settings, and a women’s cybersecurity app providing reporting tools, legal resources, and safety tips. *Social media companies, Ministry of ICT, mobile operators, and cybersecurity agencies should track adoption rates and effectiveness in reducing cyberviolence incidents.*
- Engage traditional and religious leaders to address harmful gender norms, and establish safe spaces for victims both online and offline. *Community organizations and local authorities should evaluate participation and provide feedback mechanisms to assess impact.*
- Launch national anti-cyberviolence campaigns via radio, television, and social media to increase awareness and encourage bystander action. *Monitoring and evaluation frameworks should measure reach, audience engagement, and behavioural outcomes over time.*

5.3 Future work

There is a need to conduct these studies annually because new forms of violence against women are being developed and also because more women are being exposed to ICTs as the internet penetration rates are increasing. Furthermore, future studies should include girls between three (3) and seventeen years (17) since they were not part of the study because they are below the legal age of maturity; however, these can be reached through face-to-face interviews in the presence of their guardians.

5.4 References

Al-Nasrawi, S. (2021) ‘Combating Cyberviolence Against Women and Girls: An Overview of the Legislative and Policy Reforms in the Arab Region’, in Bailey, J., Flynn, A. and Henry, N. (eds) *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Bingley: Emerald Publishing Limited, pp. 493-512. doi: 10.1108/978-1-83982-848-520211037.

Alotaibi, N.B. and Mukred, M. (2022) ‘Factors affecting the cyberviolence behaviour among Saudi youth and its relation with suicide: A descriptive study on university students in Riyadh city of KSA’, *Technology in Society*, 68, 101863.

Babbie, E. (1990) *Survey research methods*. Belmont, CA: Wadsworth.

Beran, T. and Li, Q. (2005) 'Cyber-harassment: A study of a new method for an old behaviour', *Journal of Educational Computing Research*, 32(3), pp. 265-277.

Bonanno, R.A. and Hymel, S. (2013) 'Cyber bullying and internalizing difficulties: Above and beyond the impact of traditional forms of bullying', *Journal of Youth and Adolescence*, 42(5), pp. 685-697.

Bujang MA, Omar ED, Baharum NA. (2018). A Review on Sample Size Determination for Cronbach's Alpha Test: A Simple Guide for Researchers. *Malays J Med Sci*. 25(6):85-99. doi: 10.21315/mjms2018.25.6.9.

Caridade, S., Braga, T. and Borrajo, E. (2019) 'Cyberdating abuse (CDA): Evidence from a systematic review', *Aggressive Behavior*, 48, pp. 152–168.

Chibuwe, A., & Ureke, O. (2021). 'Political trolling and the gendered nature of online harassment in Zimbabwe.' *African Journalism Studies*.

Chiome, C. (2015) 'Gender and ICTs: Women's access to ICTs in Southern Africa', *International Journal of Education and Development using Information and Communication Technology*, 11(3), pp. 1–11.

Citron, D.K. (2014) 'Addressing cyber harassment: An overview of hate crimes in cyberspace', *Case Western Reserve Journal of Law, Technology & the Internet*, 6, p. 1.

Cohen, L.E. and Felson, M. (1979) 'Social change and crime rate trends: A routine activity approach', *American Sociological Review*, 44(4), pp. 588-608.

Cyber and Data Protection Act (2021) *Cyber and Data Protection Act (Chapter 12:07)*. Harare: Government Printers.

Cybersafe (2020) *Cyberviolence against women and girls report*. Available at: <https://www.wavenetwork.org/wp-content/uploads/WP2-Report-on-Cyber-VAWG.pdf>

Dillman, D.A. (2000) *Mail and internet surveys: The tailored designed method*, 2nd ed. New York: Wiley.

Dunn, A. (2020) 'Emerging forms of online harassment and abuse: A review of recent literature', *Journal of Gender Studies*, 29(4), pp. 401-415.

Economist Intelligence Unit (EIU) (2021) *Measuring the prevalence of online violence against women*. Available at: <https://onlineviolencewomen.eiu.com/>

Einarsen, S. and Nielsen, M.B. (2015) 'Workplace bullying as an antecedent of mental health problems: A five-year prospective and representative study', *International Archives of Occupational and Environmental Health*, 88(2), pp. 131-142.

European Institute for Gender Equality (2022) *Combating Cyberviolence against Women and Girls*. Available at: <https://eige.europa.eu/publications/combating-cyber-violence-against-women-and-girls>

Fincham, J.E. (2008) 'Response rates and responsiveness for surveys, standards, and the Journal', *American Journal of Pharmaceutical Education*, 72(2), p. 43. doi: 10.5688/aj720243.

Freiheit Foundation (2023) *Zimbabwe: Cyberbullies push women to the fringes of political power*. Available at: <https://www.freiheit.org/simbabwe/cyber-bullies-push-women-fringes-political-power>

Gottschalk, F. (2022) 'Cyberbullying: An overview of research and policy in OECD countries', *OECD Education Working Papers*, No. 270. Paris: OECD Publishing. doi: 10.1787/f60b492b-en.

GREVIO (2021) *General Recommendation No 1 on the digital dimension of violence against women*. Council of Europe, Strasbourg, 20 October. Available at: <https://rm.coe.int/GREVIO-rec-no-on-digital-violence-againstwomen/1680a49147>

Hassan, E. (2006) 'Recall Bias Can Be a Threat to Retrospective and Prospective Research Designs', *The Internet Journal of Epidemiology*, 3(2).

Hassan, F.M., Khalifa, F.N., El Desouky, E.D., Salem, M.R. and Ali, M.M. (2020) 'Cyberviolence pattern and related factors: online survey of females in Egypt', *Egyptian Journal of Forensic Sciences*, 10(6). doi: 10.1186/s41935-020-0180-0.

Henson, B., Reyns, B.W. and Fisher, B.S. (2013) 'Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization', *Journal of Contemporary Criminal Justice*, 29(4), pp. 475-497.

Hinduja, S. and Patchin, J.W. (2010) 'Bullying, cyberbullying, and suicide', *Archives of Suicide Research*, 14(3), pp. 206-221.

Hinduja, S. and Patchin, J.W. (2015) *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*, 2nd edn. Thousand Oaks, CA: Sage Publications.

Hinson, L., Mueller, J., O'Brien-Milne, L. and Wandera, N. (2018) *Technology-facilitated gender-based violence: What is it, and how do we measure it?* Washington D.C.: International Center for Research on Women.

Hooks, B. (2000) *Feminist theory: From margin to center*. London: Pluto Press.

Jane, E.A. (2020) 'Online abuse and harassment', *The International Encyclopedia of Gender, Media, and Communication*, 116.

Khan, B., Shamsdin, K., Jabeen, N. and Asif, M. (2025) 'Cyberbullying and its psychological effects on secondary school students in urban Pakistan', *Journal of Social Sciences Review*, 5(1), pp. 189–196. doi: 10.54183/jssr.v5i1.483.

Kobiruzzaman, M. (2024) 'Advancing ServQual in the digital era: A framework for service responsiveness in technology-driven contexts', *Journal of Service Research and Innovation*, 12(1), pp. 55–72.

Kowalski, R.M., Giumetti, G.W., Schroeder, A.N. and Lattanner, M.R. (2014) 'Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth', *Psychological Bulletin*, 140(4), pp. 1073–1137.

Landoll, R.R., La Greca, A.M., Lai, B.S. and Chan, S.F. (2015) 'Cyber victimization by peers: Prospective associations with adolescent social anxiety and depressive symptoms', *Journal of Adolescence*, 42, pp. 77-86.

Lee, C. (2017) *Weak Commitment to School, Deviant Peers, and Cyberbullying Victimization-Strain in Adolescent Cyberbullying*. Available at: <https://search.proquest.com/pqdtglobal/docview/1937915933/abstract/9D85437600564444PQ/30>

Lee, J., Abell, N. and Holmes, J.L. (2017) 'Validation of measures of cyberbullying perpetration and victimization in emerging adulthood', *Research on Social Work Practice*, 27(4), pp. 456–467. doi: 10.1177/1049731515578535.

Lewis, H., Jones, S. and Davies, M. (2019) 'A feminist approach to online gender-based violence', *Feminist Media Studies*, 19(5), pp. 601-616.

Lewis, R., Rowe, M. and Wiper, C. (2019) 'Online abuse of feminists as an emerging form of violence against women and girls', *British Journal of Criminology*, 59(2), pp. 369–389. doi: 10.1093/bjc/azy048.

Mabika, M. and Dube, B. (2017) 'Understanding the prevalence and forms of cyber bullying at UNIVEN: A pilot study', *Online Journal of Communication and Media Technologies*, 7(1), pp. 174–190. doi: 10.29333/ojcm/2586.

Machiri, T., & Maphosa, N. (2024). 'Intersectional vulnerabilities: Digital access and online risks for rural women with disabilities in Zimbabwe.' *Journal of Gender and Digital Societies*.

Malanga, D.F. (2021) 'Survey of cyberviolence against women in Malawi', *Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development*.

Marwick, A.E. and Boyd, D. (2014) 'Networked privacy: How teenagers negotiate context in social media', *New Media & Society*, 16(7), pp. 1051–1067.

Mhlanga, D. (2022). 'Social media adoption and digital safety practices among young women in urban Zimbabwe.' *Zimbabwe Journal of Media and Communication Studies*.

Moffat, B. (2024) 'An examination of cyberbullying among Zimbabwean female social media influencers', *Online Journal of Communication and Media Technologies*, 14(4), e202451.

Moffat, P. (2024) 'Digital rights and women's online safety in Zimbabwe', *Zimbabwean Journal of Human Rights*, 14(1), pp. 22-38.

Moyo, L., & Sibanda, M. (2023). 'Between promise and practice: Assessing the enforcement of the Cyber and Data Protection Act in Zimbabwe.' *Southern African Journal of Policy and Development*.

Musawo, T. and Makoni, C. (2021) *Analysis of Cyberlaws in Zimbabwe: A Note on the Cyber Security & Data Protection Bill*. MMM Legal Practitioners. Available at: <https://www.mmmlawfirm.co.zw/analysis-cyberlaws-zimbabwe-note-cyber-security-data-protection-bill/>

Navarro, R., Yubero, S. and Larrañaga, E. (2019) *Cyberbullying across the globe: Gender, family, and mental health*. Cham, Switzerland: Springer.

Ncube, G. and Yemurai, G. (2020) 'Discrimination Against Female Politicians on Social Media: An Analysis of Tweets in the Run-Up to the July 2018 Harmonised Elections in Zimbabwe', in *Social Media and Elections in Africa, Volume 2*. Cham: Springer. Available at: https://link.springer.com/chapter/10.1007/978-3-030-32682-1_4

Noble, S.U. (2018) *Algorithms of oppression: How search engines reinforce racism*. New York: New York University Press.

OECD (2017) *PISA 2015 Results (Volume III): Students' Well-Being*. Paris: OECD Publishing. doi: 10.1787/9789264273856-en.

Olasanmi, O.O., Agbaje, Y.T. and Adeyemi, M.O. (2020) 'Prevalence and Prevention Strategies of Cyberbullying among Nigerian Students', *Open Journal of Applied Sciences*, 10(06), pp. 351–363. doi: 10.4236/ojapps.2020.106026.

Olweus, D. and Limber, S.P. (2018) 'Some problems with cyberbullying research', *Current Opinion in Psychology*, 19, pp. 139-143. doi: 10.1016/j.copsyc.2017.04.012.

Poulpunitha, D.S., Manimekalai, P.K. and Veeramani, D.P. (2020) ‘Strategies to Prevent and Control of Cybercrime against Women and Girls’, *International Journal of Innovative Technology and Exploring Engineering*, 9(3), pp. 609–612. doi: 10.35940/ijitee.k2408.019320.

Saleem, S., Khan, N.F. and Zafar, S. (2021) ‘Prevalence of cyberbullying victimization among Pakistani Youth’, *Technology in Society*, 65, 101577. doi: 10.1016/j.techsoc.2021.101577.

Sheikh, M.M.R. and Rogers, M.M. (2024) ‘Technology-facilitated sexual violence and abuse in low and middle-income countries: A scoping review’, *Trauma, Violence, & Abuse*, 25(2), pp. 1614-1629. doi: 10.1177/15248380231191189.

Sibanda, M. (2020) ‘Cyberbullying in Higher and Tertiary Education institutions in Zimbabwe: Forms, Extent, Effects and Contributing Factors’, *Journal of Systems Integration*, 11(2), pp. 217-227. doi: 10.20470/jsi.v11i2.387.

Smoktunowicz, E., Baran, T. and Boyle, M.H. (2020) ‘Beyond the bully-victim dichotomy: The role of self-labelling and self-report measures of victimization and bullying in predicting long-term negative outcomes’, *Journal of Youth and Adolescence*, 49, pp. 143-162.

Tourangeau, R. and Yan, T. (2007) ‘Sensitive questions in surveys’, *Psychological Bulletin*, 133(5), p. 859.

Wang, J., Iannotti, R.J. and Luk, J.W. (2018) ‘Patterns of adolescent bullying behaviours: Physical, verbal, exclusion, rumour, and cyber’, *Journal of School Psychology*, 69, pp. 77-88.

Zimbabwe Data Protection Act (2021) [Chapter 11:12]. Available at: <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/114001/143076/F-26458745/ZWE114001.pdf>

ZIMSTAT (2020) *2020 Information and Communication Technology (ICT): Access By Households And Use By Individuals Survey Report*. Harare: ZIMSTAT.

ZIMSTAT (2022) *Zimbabwe 2022 Population and Housing Census*. Harare: ZIMSTAT.