Pakistan Journal of Psychological Research, 2024, Vol. 39, No. 4, 875-894

https://doi.org/10.33824/PJPR.2024.39.4.47

Construction and Validation of Cyber Harassment Experience Scale (CHES)

Sumaira Ayub and Farah Malik

University of the Punjab

The aim of this study was to develop indigenous, valid, and reliable measure to assess the experiences of cyber harassment in young women. An initial item pool of 69 items was generated through focus group discussion, in-depth interviews with victims and experts dealing with cases of cyber harassment including Cyber Crime Wing, Judges, lawyers, and experts from NGOs. A preliminary scale was administered to a sample of 365 young women, aged between 18 and 30 years (M = 20.81, SD = 2.71), from four public and private sector universities in Lahore. The participants were selected using a purposive sampling strategy. Principal component analysis with Varimax rotation postulated 54 items with four factors named as unauthorized use of identity information, use of sexual content, cyber terrorization, and intimidation that accounted 66.74% variance. Cronbach's alpha for the final scale was .98 and ranged .86 to .98 for the emerged factors. The results indicated that CHES is a reliable and valid measure for assessing experiences of cyber harassment in young women. This study may be helpful for the development and evolution of programs designed to alleviate harassing behaviors in cyber space considering the severity of the issue

Keywords. Cyber harassment, unauthorized use, identity information, sexual content, cyber terrorization, intimidation, young women, principal component analysis

Cyber harassment refers to unwelcome behaviors that degrade, intimidate, or offend a victim, leading to a hostile environment for the victim. Cyber harassers target their victims through chat rooms, message boards, discussion forums, and emails. The hostile environment can be created through persistent misbehavior or a single incident (Milhorn, 2007). Cyber harassment encompasses various forms of harmful behavior, including threats of violence, invasions of privacy, spreading false and damaging information about the victim,

Sumaira Ayub and Farah Malik, Institute of Applied Psychology, University of the Punjab, Lahore, Pakistan.

Correspondence concerning this article should be addressed to Sumaira Ayub, Institute of Applied Psychology, University of the Punjab, Lahore, Pakistan. Email: sumairaayub002@gmail.com

urging strangers to physically harm the victim, and carrying out technological attacks. It can also involve malicious actions such as creating fake online advertisements that disclose the victim's contact information and offer them to involve in sexual activities. Additionally, perpetrators may seek revenge by posting the victim's intimate or nude photos on websites without their consent (Citron, 2014; Jain, 2005). So, it is meant to include a variety of online actions: cyber stalking, bullying, flaming, trolling, intimidation, blackmail, exclusion, extortion, Impersonation or masquerading, revenge porn, and the invasion of privacy (Beale & Hall, 2007; Mohsin, 2016; Willard, 2006). Cyber harassment looks very much like face-to-face harassment, but the drastic difference between cyber harassment and face-to-face harassment is, anonymity, and therefore the willingness for the offender to take risks and act with abandonment and viciousness (Strauss, 1990).

The Internet offers a level of anonymity that enables individuals to engage in criminal activities, such as cyber harassment, to express their desire for seeking revenge or enjoyment in causing harm to others. This virtual outlet allows them to freely express their hatred without immediate consequences. The main reason for harassing behavior is that the perpetrators are motivated by the desire to control the victims (Bocij, 2004). Dominance theory suggests that people who have a strong desire for power and control are more likely to engage in cyber bullying and cyber harassing behaviors. According to Olweus (1994), harassers often display a pattern of aggression, particularly in the case of boys, which may be combined with physical strength. However, he also highlighted that dominance or leadership status can be established not only through physical strength but also through verbal abuse, threats, and other intimidating behaviors, including sexually aversive actions. These behaviors are driven by the individual's need for power, control, and social status. Therefore, the internet can serve as a means for individuals to assert dominance and exert control over others (Campfield, 2006). The cyber harasses/ bullies are having maladaptive self-esteem (defensive egotism, implicit self-esteem, narcissism, and defensive self-enhancement) that is strongly linked to aggression, so they use aggressive behaviors on internet or cell phone to restore, regulate and enhance their self-esteem (Baumeister et al., 2003).

Females are more likely to be harassed on cyber space and they are more likely to experience indirect forms of cyber harassment including receiving “prurient, lewd and sexually explicit messages” (Strauss, 2013), the harassers are males, and they are motivated by the desire to control the victims (Bocij, 2004). Most of the harassers have

been in a relationship with their victims, they are either boyfriend or ex-boyfriend, acquaintances, or in a victim-offender relationship and friend or former friend (Reyns, 2010). In Lenhart and Madden's (2007) opinion, the inappropriate sharing of personal information can put young people at significant risk of victimization, while also harming their future job prospects and college admissions. The schoolyard bully, the jealous friend, boyfriend or ex-boyfriend, the boss hiding feelings of inferiority by putting down his employees, or the numerous cases throughout history of people persecuting, assaulting, and harassing those who live outside the status quo may also be the reasons (Gardener, 2019; Reyns, 2010).

Cyber-harassment causes victims to experience physical or emotional stress, a sense of helplessness, fear for victims, and even suicide (Bocij, 2004; Finn, 2004). People who are cyberbullied suffer from innumerable problems, including constant dread, fear, low self-esteem, and depression (Parks, 2013). According to Hinduja and Patchin (2012) as they stated experience of being victimized decreases one's self-esteem; individuals with lower self-esteem are more susceptible to becoming targets of cyber victimization. The harassing behaviors and actions cause victims to experience intimidation, as well as psychological and emotional distress (National Response Center for Cyber Crime, 2016). The psychological effect of cyber harassment on victims can produce an intense and prolonged fear. This fear usually includes an increasing fear of the escalation of the frequency and nature of the conduct (for example, from non-violent to life-threatening) and is accompanied by a feeling of loss of control over the victim's life. Majority of the incidents ranged from annoying to the occurrence of death threats (Beran & Li, 2005). Depression, emotional distress, poor academic performance, and low self-esteem have been found to be linked to online harassment (Barren & Li, 2005; Hafeez, 2014; Valkenburg et al., 2006; Willard, 2006; Ybarra, 2004), the victims also develop insecurities and have decreased social ties (Hiduja & Patchin, 2007).

In Pakistan it is highly under reported offence. Cultural norms and the idea of "honor" may be a reason for victims not to seek help and report harassment. However, on a more basic level, due to lack of awareness and education about cyber harassment and "how to seek help" is also the reason (Mohsin, 2016). According to Magsi et al. (2017), approximately 45 percent of victims of cyber harassment choose not to disclose such incidents to their families due to the fear of being labeled as immoral. As a result, young women opt to suffer silently, which not only hinders their ability to utilize online platforms freely but also disrupts their personal lives. Furthermore, individuals

who have been subjected to cyber harassment not only exhibit a lack of trust in law enforcement agencies but also possess limited knowledge regarding the existing laws against cyber harassment. The extent of cybercrime in Pakistan can be understood by examining the number of complaints received across various categories. In 2020, the FIA received a total of 84,764 complaints. Among these, a significant portion consisted of 20,218 complaints related to financial fraud, 7,966 complaints regarding hacking, 6,023 complaints related to cyber harassment or threats, 4,456 complaints concerning fake profiles or identity theft, 6,004 complaints of defamation, 3,447 complaints regarding cyber blackmailing, and 892 complaints of hate speech.

Researchers had so far focused on measuring the experiences of cyber bullying in adolescents, the consequences, and their coping. Literature suggests that there are some differences in experiences of cyber harassment in young adults and they differ in their coping responses. Furthermore, culture plays a very important role in labeling behaviors as harassing or not. Previously there was no standardization to explore the experiences of cyber harassment in young female university students in Pakistani cultural context. So, this study is important in constructing an indigenous measure of Cyber Harassment Experience Scale (CHES) by engaging victims and experts of the field.

Objectives of the Study

1. To develop an indigenous scale to assess experiences of cyber harassment in young women.
2. To determine the psychometric properties for Cyber Harassment Experience Scale (CHES).

Method

The development and validation of the CHES was carried out in two phases. In phase 1 incorporated construction and validation of the scale; however, Phase II included determining psychometric properties of the newly developed measure.

Phase I: Development and Validation of Cyber Harassment Experience Scale (CHES)

Phase I was proposed to develop the CHES and consisted of two steps. The first step was intended to generate item pool for scale with the help of young female university students, victims, and expert

dealing cyber harassment issues by using open-ended questionnaires. Hence the item pool was generated. The finalized items were analyzed through factor analysis to establish the factorial structure of the final instrument.

Step 1: Construct Identification and Item Generation

For the sake of item generation and formulation, in-depth interviews and focus group discussion were conducted.

Focus Group. A focus group with eight participants (n = 8) of age range 24-28 years including MPhil (n = 6) and PhD (n = 2) scholars was conducted to explore the construct regarding experiences of cyber harassment following ethical guidelines. The discussion was audio recorded then it was transcribed by the researchers and verbatims were identified.

Interviews. Moreover, in-depth interviews from eight victims (n = 8) of cyber harassment were also taken. The victims were contacted through social media and were interviewed after having their verbal consent. The interviews were recorded and transcribed by the researchers and verbatim were identified. The confidentiality of the recorded information was ensured to all the participants.

Expert Opinions. Moreover, eight experts from the field of cybercrimes i.e., Cybercrime Wing- FIA (n = 2), judges and lawyers of High Court and Session Court (n = 3), Digital Right Foundation-NGO (n = 2) and Cyber Law intelligence international- NGO (n = 1) were also approached and interviewed to enrich the item pool.

During each interview/discussion/expert opinion prompts were given to them for further exploration about the experiences of cyber harassment. Respondent's responses were audio recorded. All the recordings were then transcribed by the researchers and verbatim were identified. After this the general pool of 69 items was formulated. Then the formulated items were administered to the MPhil (n = 4) and PhD (n = 3) scholars to ensure the content validity of the items. A few of the items were modified and added further. After that it was properly discussed with the supervisor and further amendments were made to the items. So, after amendments, the final 69 items were retained for empirical evaluation.

Step 2: Tryout

The questionnaire was then administered on 20 female university students of age range 19- 30 years for items try out. The scale was administered to participants who showed their willingness to participate in the study. They were given brief instructions before filling the questionnaire. They were asked to rate the statement for which they feel that it is more appropriate for them. The responses were given on 5-point Likert scale (1 = *Never*, 2 = *One or Two Times*, 3 = *Sometimes*, 4 = *Often*, 5 = *Mostly*). The data obtained were then analyzed by the researcher. After analysis and feedback from participants it was ensured that none of the items needed any improvement. So, this version was retained and used for the next phase for validation.

Phase II: Determining the Psychometric Properties of CHES

Phase II of scale development was to run factor analysis, to determine scoring procedure, cut off and to conduct reliability analysis. Factor analysis was used to identify the underlying factor structure of the items in the final CHES scale. Percentile ranks were employed to establish cut-off points, and a reliability analysis was conducted to evaluate the internal consistency using alpha coefficient.

Sample

It is widely acknowledged that a larger sample size is considered more reliable for validating a measure. Tabachnick and Fidell (2013) stated that it is reassuring to have a minimum of 300 cases for factor analysis (p. 613). Additionally, it is recommended that the sample size meets the criteria of 5:1, meaning there should be at least five cases per item. For the empirical evaluation a sample of 365 female university students of age range 19-30 years (M = 20.81, SD = 2.71) was taken from four universities of city Lahore considering public and private sectors both. Sample was drawn using purposive sampling strategy. Those female students who were active internet users and had any experience of cyber harassment were included.

Procedure

The study was approved by the departmental committee. To collect data, the necessary permissions were obtained from the relevant authorities by submitting a letter issued by the department.

The participants were approached and were briefed about the nature and purpose of the study. All the ethical considerations were followed such that written consent was taken ensuring confidentiality of their information, volunteer participation, right to withdraw at any stage when they feel harm. It took 5-7 minutes on average to fill the questionnaire. For the current study, a total of 420 female students were initially contacted. However, after screening, 365 participants were included in the analysis. A total of 55 questionnaires were excluded from the data due to poor data quality, such as patterned responses, rushed responses, or incomplete information. Therefore, the overall response rate for the study was 86.90%.

Results

To establish construct validity, Principal Component Analysis (PCA) was used followed by Varimax rotation method was used. To determine whether the data was appropriate for factor analysis, several assumptions were empirically tested. Researchers have explored various options for evaluating sampling adequacy. One method used to assess sample adequacy is the Kaiser-Mayer-Olkin (KMO) measure. Kaiser (1960) recommended a minimum value KMO for sample adequacy is .50 (.50 - .70 = mediocre, .70 - .80 = good, .80 - .90 = great and above .90 = superb). KMO value for the current analysis was .97, thus defining the sample adequacy as superb. Bartlett's Test of Sphericity was observed as highly significant, χ^2 (29171.36) = $p < .001$ which indicated that correlation between the items was sufficiently large for PCA (Hutcheson & Sofroniou, 1999). So, based on Table 1, factor analysis was found suitable.

Table 1: *Kaiser-Mayer Test for Sampling Adequacy and Bartlett's Test of Sphericity (N = 365)*

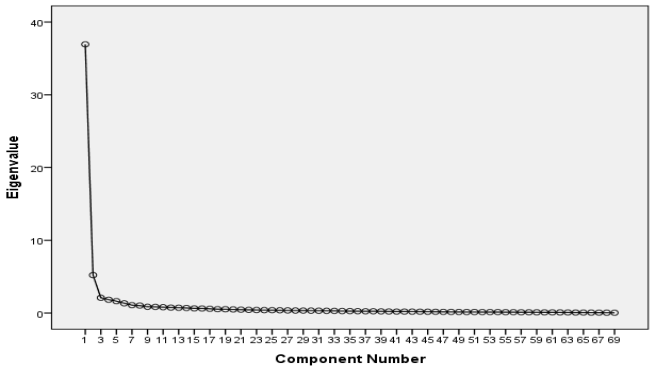
Kaiser- Mayers-Olkin Test for Sampling Adequacy	.97
Bartlett's Test of Sphericity, Approx. χ^2	29171.36***
Df	2346

Note. *** $p < .001$.

To determine the appropriate number of components (factors) to extract, there was a need to consider a few pieces of information provided in the output. Using criteria given by Kaiser (1960) the only that factor was considered which was having Eigen value > 1. In addition to the criteria based on eigenvalues, Cattell's (1966) scree plot was also utilized to determine the number of factors. According to

Cattell's criteria, factors that are located above the "elbow" of the plot were retained (Figure 1).

Figure 1: *Scree Plot Emerged from Exploratory Factor Analysis*



After analyzing the Scree plot, it was decided to rerun the factor analysis with four suppressions by employing principal component analysis with Varimax rotation. The factor loading of .45 and above was followed (Tabachnick & Fiddell, 2007). Based on this factor loading criteria, 54 out of 69 items were retained. The results are discussed in Table 2.

Table 2: *Factor Structure and Item Analysis for Cyber Harassment Experience Scale (N = 365)*

Sr. #	Items #	Item Verbatim	Loadings				r^{it}
			1	2	3	4	
1	16	Someone blackmailed me by photo shopped…	**.73**	.26	.31	.05	.75
2	17	Someone posted my photo shopped pictures on dirty…	**.78**	.18	.24	.10	.75
3	18	Someone stole my personal information and posted on…	**.66**	.11	.31	.26	.71
4	24	Someone spread false information about me on…	**.52**	.21	.37	.36	.72
5	25	Someone stole my identity-related information…	**.57**	.15	.33	.41	.74
6	26	Someone created and used multiple fake accounts using…	**.62**	.13	.26	.36	.71
7	27	Someone created fake social media …	**.70**	.21	.16	.40	.78
8	28	Someone blackmailed me by stealing…	**.65**	.32	.17	.35	.79

Continued…

Sr. #	Items #	Item Verbatim	Loadings				r^{it}
			1	2	3	4	
9	29	Someone created my fake account and posted….	**.80**	.23	.08	.24	.77
10	30	Someone posted sexually explicit videos by…	**.80**	.28	.13	.12	.77
11	31	Someone posted my personal life information by …	**.76**	.33	.17	.17	.80
12	32	Someone posted my private pictures by …	**.78**	.22	.13	.23	.76
13	33	Someone distressed me using my personal ….	**.56**	.28	.20	.44	.75
14	36	Someone posted my pictures along with my phone number…	**.80**	.31	.16	.05	.77
15	37	Someone stole my personal information and uploaded on….	**.75**	.35	.22	-.00	.76
16	41	Someone offered me to show himself nude on …	**.50**	.43	.26	.42	.80
17	44	Someone blackmailed me by taking my personal ….	**.72**	.07	.18	.30	.70
18	45	Someone took my personal photos and other….	**.80**	.10	.20	.31	.79
19	46	Someone misused my personal…	**.77**	.16	.12	.29	.75
20	47	Someone hacked my email or other social media….	**.58**	.30	.16	.33	.72
21	48	Someone misused my email or other…	**.73**	.35	.08	.23	.77
22	49	Someone posted my personal videos on…	**.78**	.38	.09	.02	.74
23	50	Someone stole my personal videos and posted on…	**.79**	.38	.12	.03	.77
24	51	Someone made my personal videos…	**.79**	.35	.05	.09	.74
25	52	Someone posted my pictures and phone number on ….	**.76**	.41	.09	.01	.74
26	62	Someone sent my edited pictures to…	**.79**	.24	.06	.31	.78
27	63	Someone posted my edited pictures on…	**.80**	.18	.09	.34	.78
28	64	Someone sent my edited pictures to my friends…	**.79**	.19	.15	.31	.80
29	65	Someone updated the cover page of the social media account by…	**.80**	.21	.16	.27	.80
30	67	My boyfriend/ fiancé threatened me over…	**.56**	.43	.10	.31	.72
31	11	Someone sent me sexually suggestive messages…	.31	**.66**	.36	.25	.76

Continued…

Sr. #	Items #	Item Verbatim	Loadings 1	2	3	4	r^{it}
32	12	Someone sent me dirty'/immoral messages…	.21	**.63**	.41	.26	.70
33	13	Someone sent me obscene pictures…	.27	**.63**	.39	.21	.71
34	14	Someone sent me obscene videos…	.43	**.59**	.35	.24	.80
35	15	Someone sent me pictures of sex organs…	.38	**.59**	.38	.18	.75
36	21	Someone made a compliment on my body shape by …	.37	**.59**	.35	.26	.77
37	22	Someone commented on my body over…	.39	**.64**	.33	.24	.78
38	54	Someone deliberately made fun of me on ….	.37	**.60**	.14	.32	.70
39	55	Someone made sexually explicit comments on my post …	.43	**.64**	.08	.37	.75
40	66	Someone made sexually explicit comments on my post …	.40	**.50**	.14	.37	.69
41	1	Someone disturbed me by calling from….	.02	-.12	**.80**	.11	.31
42	2	Someone disturbed me through messages….	.05	-.07	**.79**	.08	.33
43	3	Someone annoyed me with too many messages on...	.12	.33	**.62**	.14	.46
44	6	Someone called me repeatedly by changing….	.15	.29	**.69**	.17	.57
45	7	Someone repeatedly sent me messages by …	.06	.30	**.71**	.17	.52
46	8	When I blocked a number, someone….	.20	.32	**.66**	.19	.61
47	9	Someone annoyed me with calls/ messages from a new account …	.29	.40	**.59**	.26	.71
48	10	Someone sent me threatening messages on...	.41	.42	**.55**	.14	.74
49	34	Someone annoyed me with offensive comments…	.19	.29	.36	**.59**	.63
50	35	Someone tried to contact me by changing...	.18	.26	.36	**.61**	.61
51	38	Someone sent me indecent romantic…	.23	.41	.34	**.49**	.67
52	42	An unknown person sent me my profile or cover photos…	.38	.21	.38	**.59**	.73
53	43	An unknown person sent messages praising my profile …	.27	.21	.34	**.62**	.64

Continued…

Sr. #	Items #	Item Verbatim	Loadings 1	2	3	4	r^{it}
54	57	Someone threatened to share screenshots…	.45	.45	.14	**.46**	.73
Eigen Value			39.93	5.21	2.09	1.83	
% of Variance			53.53	7.55	3.02	2.65	
Cumulative % of Variance			53.53	61.07	64.10	66.75	
Cronbach's α			.98	.95	.90	.86	

Note. Factor Loadings > .45, r^{it} = item total correlation > .30, α= Alpha.

Factor Description

The emerged four factors were named and explained as followed:

Factor 1: Unauthorized Use of Identity Information (UUII). The Eigen values of factor 1 was 39.93 which explained 53.53% variance. It is comprised of 30 items related to misuse and damage of identity information characterized by the experiences related to obtaining, selling, possessing, transmitting, using, or destroying identity information without authorization using social media and any other platform.

Factor 2: Use of Sexual Content (USC). The Eigen value of factor 2 was 5.21 which explained 7.55% variance whereas the cumulative percentage of the variance was 61.07%. It consisted of 10 items related to receiving sexual contents on personal social accounts, characterized as experiences of receiving pornographic/sexist images, videos, messages or remarks in Messenger, WhatsApp, cell phone or in a comment on any post on social media account.

Factor 3: Cyber Terrorization (CT). Factor 3 had an eigenvalue of 2.09, which explained 3.02% of the variance. The cumulative variance accounted for by all factors up to that point was 64.10%. It comprised of 8 items measuring harassment experiences on cellular/ personal numbers and social media accounts. The items are basically related to coercing, creating sense of fear, panic or insecurity through messages and calls.

Factor 4: Intimidation (INT). The Eigen value of factor 4 reported as 1.83, with 2.65% explained variance whereas 66.75% of cumulative variance. It consisted of 6 items measuring experiences of being threatened or exposed through cell phones and social media. It measures to what extent one is being intimidated, threatened, or exposed through cell phones and social media.

Furthermore, Monte Carlo Parallel Analysis was also applied to further confirm the number of factors to be considered (Horn, 1965). The analysis generated hypothetical Eigen values are comparable with the Eigen values generated by PCA. Monte Carlo parallel analysis is not supported by SPSS, so for this analysis *Monte Carlo PCA* (a computer application) was developed by Watkins (2000) in which Eigen values from principal component analysis were compared with randomly generated Eigen value. Therefore, this separate application was downloaded, and analysis was run out.

Table 3: *Parallel Component Analysis using Monte Carlo PCA (N = 365)*

Factors	Random Eigenvalue	Eigenvalues for PCA	Decision
1	1.21	36.93	Accepted
2	1.32	5.21	Accepted
3	1.08	2.09	Accepted
4	1.02	1.83	Accepted
5	0.97	1.63	Rejected
6	0.92	1.34	Rejected
7	0.86	1.08	Rejected
8	0.79	1.02	Rejected

From Table 3, the *Monte Carlo for Parallel Analysis* indicated that four factors through principal component analysis were within the acceptable range. Moreover, the other four factors had eigenvalues for parallel analyses were lower than eigenvalues for PCA, they were rejected because of ambiguous clusters of items.

Later, the scoring procedure for the developed scale was determined.

Reliability and Item Analysis

The internal consistency of the items for CHES scale was assessed using Cronbach's alpha coefficient. The final 54-item scale reported .98 alpha reliability while its subscales have reliability ranged from .86 to .98 which falls in sufficient range (See Table 4).

Table 4: *Reliabilities and Descriptive Statistics of Study Variables (N = 365)*

Scales	*k*	*M*(*SD*)	Ranges	*α*
Cyber Harassment Experience Scale	54	89.82(39.86)	56-248	.98
Unauthorized Use of Identity Information	30	43.02(22.81)	30-134	.98
Use of Sexual Content	10	17.31(9.25)	10-46	.95
Cyber Terrorization	8	18.66(7.31)	8-40	.90
Intimidation	6	10.56(5.03)	6-28	.86

Based on the findings presented in Table 5, all four subscales demonstrated significant positive relationships with one another, as well as with the overall CHES score. The significant inter-correlations between the whole scale and its subscales indicated satisfactory construct validity.

Table 5: *Inter-Correlation Between Subscales and Total Scores of the Cyber Harassment Experience Scale*

Scales	*1*	*2*	*3*	*4*	*5*
Unauthorized Use of Identity Information	-	.78**	.53**	.72**	.94**
Use of Sexual Content		-	.71**	.78**	.91**
Cyber Terrorization			-	.68**	.75**
Intimidation				-	.85**
Cyber Harassment Experience Scale					-

Note. ** $p < .01$.

Scoring Procedure

Cut off scores were determined by using percentile rank method to differentiate among the levels (mild, moderate, moderately severe, and severe) of experiences of cyber harassment. Percentiles or percentile rank were used interchangeably, and it is the most common type of norm development for psychological test, and widely used to derive scores because of their ease of interpretation (see Table 6).

Table 6: *Categories of Cyber Harassment Experience Scale (N = 365)*

Percentiles	Levels	Raw Score	*f* (%)
25	Mild	>64	97 (26.6)
50	Moderate	65-76	91 (24.9)
75	Moderately Severe	77-102	88 (24.1)
100	Severe	103-248>	89 (24.4)

Note. CHES = Cyber Harassment Experience Scale.

Table 6 revealed categories for the scores on Cyber Harassment Experience Scale (CHES). These categories of scores can be labeled as Mild experiences of cyber harassment when score is > 64 on 25th percentile, moderate experiences when score is in the range of 65-76 with 50th percentile, moderately severe experiences when score falls in the range of 77-102 with 75th percentile, and severe experiences when the score is in the range of 103-248 > with 100th percentile rank. Moreover, frequency and percentage of level of cyber harassment were check out for respondents that indicated about 26.6% respondents showed mild level of cyber harassment, 24.9% of moderate level, 24.1% of moderately severe experiences of cyber harassment and 24.4% showed severe level of cyber harassment.

Discussion

The present study aimed at studying the phenomenon of cyber harassment in Pakistan. To achieve the objectives, an indigenous instrument was required which could measure the various experiences related cyber harassment in young women. Therefore, Cyber Harassment Experience Scale (CHES) was developed. To assess the construct validity of the scale, Principal Component Factor Analysis with Varimax rotation was conducted. Four factors named as Unauthorized Use of Identity Information (UUII), Use of Sexual Content (USC), Cyber Terrorization (CT) and intimidation (INT) were emerged and retained based on factor loading criteria to use a loading of .45 by Tabachnick and Fidell (2007). Thus, items were considered to load strongly on a particular factor if the loading was ≥ 45 and they were mutually exclusive on one factor. Based on multiple criteria, including Eigenvalue greater than 1, Monte Carlo parallel analysis, Scree plot, having no factors with fewer than three items, and theoretical relevance (as recommended by Hair et al., 2010; Kline, 2013), all four factors were selected for further analysis. The Cyber Harassment Experience Scale (CHES) appeared as a multidimensional and unique measure in terms of content as its sub-scales revealed four domains of experiences of cyber harassment in young women.

The first factor named as “Unauthorized Use of identity information” measures the experiences related to obtaining, selling, possessing, transmitting, using, or destroying identity information without authorization. For example, “Someone blackmailed me by modifying my pictures through photoshop (making them obscene and nude), someone put me in severe stress by posting my photoshopped pictures on “dirty” sites” etc. Identity theft via social media has emerged as a rapidly escalating global crime. A significant number of individuals remain oblivious to the extent of personal information they

inadvertently share across various internet platforms, including social media and social networking sites (Salman, 2020). This is growing issue faced by young women in Pakistan. According to the perspective of conflict theory given by Hutchinson et al. (2010), bullying is rooted in inequality, power imbalances, and oppression. It posits that bullying behavior arises because of a power struggle or quest for dominance between individuals occupying different positions on the social hierarchy. This struggle for supremacy can ultimately manifest as bullying behavior.

The factor two named as "Use of Sexual Content" measures experiences of receiving pornographic/sexist images, videos, messages or remarks in Messenger, WhatsApp, cell phone or in a comment on any post on social media. For example, "Someone sent me pictures of sex organs/genitals on Facebook / WhatsApp, someone sent me sexually explicit messages on Facebook, someone sent me offensive 'dirty'/ immoral messages on Facebook" etc. This subscale is somehow comparable to cyber sexual harassment scale given by Schenk (2008), which is linked to negative experiences related to uninvited sexual attention as well as sexual coercion that made someone feel uncomfortable, awkward, or unsafe. The types of cyber sexual harassment, which are mostly reported in different studies are unwanted sexual solicitation, receiving unwanted sexual messages/ images, and having sexual texts/images shared without permission (Reed et al., 2020). Researchers have provided a comprehensive definition of cyber sexual harassment, describing it as a wide array of sexually explicit or harassing images, messages, or content that is transmitted and disseminated through digital mediums. This includes activities such as sending unsolicited explicit messages, sharing explicit photos without consent, engaging in online sexual coercion, or any other form of digital communication that aims to demean, intimidate, or exploit individuals in a sexual context (Henry & Powell, 2018; Madigan et al., 2018). According to a study conducted by Duggan in 2017, it was discovered that 21% of women between the ages of 18 and 29 reported experiencing online sexual harassment. In contrast, only 9% of men within the same age range reported similar experiences.

The factor three named as "Cyber Terrorization" basically related to coercing, creating sense of fear, panic or insecurity through messages and calls. For example, " Someone repeatedly annoyed me by calling through changed phone number, someone sent me threatening messages based on personal information on WhatsApp/ Facebook Messenger" etc. Cyber terrorization is common experience among young women in such that to combat this**,** there is a clause in

Prevention of Electronic Crime Act (2016). For instance, it describes any action or behavior intended to force, intimidate, create fear, panic, or insecurity within the government, the public, a specific community, sect, or society as a whole. It encompasses any behavior that seeks to create a climate of fear or insecurity within a given social context. Although there is option of blocking the contacts, but the receiving calls at odd times with odd numbers could be more panicking rather inviting.

Factor four is named "Intimidation" which measures to what extent one is being intimidated, threatened, or exposed through cell phones and social media. For example, "Someone threatened me to spread the screenshots of my gossip with him, someone tried to contact me by repeatedly changing accounts on Facebook" etc. This is also most prevalent experience in young women many of the young women experiencing it a lot which suffer their mental health. This subscale is comparable to Real-life transfer and threat subscales of Cyber-Obsessional Pursuit (COP) Scale given by Spitzberg et al. (2001), the items related to meeting first online and then following in real world and sending threatening messages. This subscale is somehow also to the concept of cyberstalking given Bocij (2002) and Finn (2004), who state that series of behaviors and actions carried out consistently over a period of time, with the intention of intimidating, alarming, frightening, or harassing the victim and also their family, partner, and friends. These persistent actions aim to create a hostile and distressing environment for the victims and for those who are close to them.

Based on above discussion, it could be concluded that all the factors of the CHES are appropriately well defining the phenomenon of experiences of cyber harassment in young women, also it showed significant inter-correlations between the whole scale and it and its subscales depicting adequate construct validity, further all the four factors showed significant internal consistency. So, CHES is proved to be a reliable and valid measure to study the experiences of cyber harassment in Pakistan as well as in other cultures too.

Limitation and Suggestions

A gross limitation of this study was found regarding the response of the participants. Many of the participants responded in a socially desirable manner. So, in future studies measures should be taken to mitigate the influence of socially desirable factors. Furthermore, it is important to note that the study exclusively included female participants. To enhance the generalizability of the findings, future

research should aim for a more diverse sample by including participants of different genders. Further a comparative study can also be conducted on the sample of other genders to study the nature and extent of experiences of cyber harassment.

Implications and Recommendations

This study was important in constructing a tool to measure experiences of cyber harassment. Further in future CHES may be useful for increasing understanding of experiences of cyber harassment. The purpose of this study is to contribute to the field of criminal and forensic psychology by providing valuable research that can facilitate easier measurement of the variables involved. By conducting this research, it is anticipated that a better understanding of the phenomenon will be gained, leading to more effective interventions and strategies to combat cyber harassment. Media outlets and opinion-makers should also come forward to highlight this issue and spread awareness. In educational institutions the students should be taught about internet safety, rights of privacy and freedom of expression, and methods to report and cope. Due to cultural norms this issue is highly under reported. The idea of honor may be the reason to not seek help. Parents should bring up their children in such a way that when they face this issue, they may stand against it rather than avoid it. Additionally, parents should maintain vigilant oversight of their children's internet activities to ensure their safety and provide guidance when necessary.

References

Baumeister, R. F., Smart, L., & Boden, J. M. (1996). Relation of threatened egotism to violence and aggression: The dark side of high self-esteem. *Psychological Review, 103*(1), 5-33.

Beale, A. V., & Hall, K. R. (2007). Cyberbullying: What school administrators (and parents) can do? *The Clearing House: A Journal of Educational Strategies, Issues and Ideas, 81*(1), 8-12. https://doi.org/10.3200/TCHS.81.1.8-12

Beran, T., & Li, Q. (2005). Cyber-harassment: a study of a new Method for an old behavior. *Journal of Educational Computing Research, 32*(3), 265-277. https://doi.org/10.2190/8YQM-B04H-PG4D-BLLH

Bocij, P. (2002). Corporate cyberstalking: An invitation to build theory. *First Monday, 7(*11). https://doi.org/10.5210%2Ffm.v7i11.1002

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet Age and how to Protect Your Family*. American Library Association: Praeger Publisher.

Campfield, D. C. (2006). *Cyber bullying and victimization: Psychosocial Characteristics of bullies, victim, and bullied victim* [Master's dissertation, University of Montana].

Cattell, R. L. (1966). The Scree test for number of factors. *Multivariate Behavioral Research, 1,* 245-276.

Citron, D. K. (2014). *Hate Crimes in Cyberspace*. Harvard University Press.

Clarke, R.V. (2004). Technology, criminology, and crime science. *European Journal on Criminal Policy and Research, 10,* 55-63. https://doi.org/10.1023/B:CRIM.0000037557.42894.f7

Duggan, M. (2017, July 11). *Online harassment 2017*. Retrieved from http://www.pewinternet.org/2017/07/11/online-harassment-2017

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19*(4), 468-475. https://doi.org/10.1177/0886260503262083

Gardner, D. (2019). The rise of cyberstalking and online harassment. *Today's Insurance Professionals, 76*(1), 31-35.

Hafeez, E. (2014). Cyber harassment and its implications on youth in Pakistan. *New Horizons, 8*(2), 29-48.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis: A global perspective.* Pearson.

Henry N., & Powell A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence & Abuse, 19,* 195-208. https://doi.org/10.1177/1524838016650189

Patchin, J. W., & Hinduja, S. (2012). Cyber bullying: An update and synthesis of the research. In *Cyber bullying prevention and response* (pp. 13-35). Routledge.

Horn, J. L. (1965). A rationale and test for number of factors in factor analysis. *Psychometrika, 30,* 179-185. https://doi.org/10.1007/BF02289447

Hutcheson, G., & Sofroniou, N. (1999). *The multivariate social scientist introductory statistics using generalized linear models.* Thousand Oaks, Sage Publication.

Hutchinson, M., Vickers, M. H., Jackson, D., & Wilkes, L. (2010). Bullying as circuits of power: An Australian nursing perspective. *Administrative Theory & Praxis, 32*(1), 25-47. https://doi.org/10.2753/ATP1084-1806320102

Jain, A. (2005). *Cyber Crime: Issues, Threats, and Management* (2nd ed). Isha books.

Kaiser, H. F. (1960). The application of electronic computers factor analysis. *Educational and Psychological Measurements, 20,* 141-151.

Kline, P. (2013). *Handbook of Psychological Testing*. Routledge.

Lenhart, M., & Madden, M. (2007). Teens, Privacy and Online Social Networks Pew Research Center: Internet, Science & Tech. United States of America. https://coilink.org/20.500.12592/fr0rcw

Madigan S., Ly A., Rash C., Van Ouytsel J., & Temple J. (2018). Prevalence of multiple forms of sexting behavior among youth. *JAMA Pediatrics*, *172*, 327-335. https://doi.org/10.1001/jamapediatrics.2017.5314

Magsi, H., Agha, N., & Magsi, I. (2017). Understanding cyber bullying in Pakistani context: Causes and effects on young Female university students in Sindh Province. *New Horizons*, *11*(1), 103-110.

Milhorn, T. H. (2007). *Cybercrime: How to Avoid Becoming a Victim*. Universal-Publishers.

Mohsin, M. (2016, April 16). The cyber harassment of women in Pakistan. *The Diplomat.* Retrieved from http://thediplomat.com/2016/04/the-cyber-harassment-of-pakistans-women/

National Response Center for Cyber Crimes. (2016). *Cyber Crimes*. Retrieved from http://www.fia.gov.pk/en/NR3C.php

Olweus, D. (1994). Annotation: Bullying at school: Basic facts and effects of a school-based intervention program. *Child Psychology & Psychiatry & Allied Disciplines*, *35*(7), 1171-1190. https://doi.org/10.1111/j.1469-7610.1994.tb01229.x

Parks, P. J. (2013). *Cyber Bullying.* Reference Point Press, Inc.

Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyber bullying. *Youth Violence and Juvenile Justice*, *4*(2), 148-169. https://doi.org/10.1177/1541204006286288

Patchin, J., & Hinduja, S. (2010). Changes in adolescent online social networking behaviors from 2006 to 2009. *Computers in Human Behavior*, *26*, 1818-1821. https://doi.org/10.1016/j.chb.2010.07.009

Reed, E., Wong, A., & Raj, A. (2020). Cyber Sexual Harassment: A Summary of Current Measures and Implications for Future Research. *Violence against women*, *26*(12-13), 1727-1740. https://doi.org/10.1177/1077780121988095

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention & Community Safety*, *12*, 99-118. https://doi.org/10.1057/cpcs.2009.22

Salman, H. M. (2020). Identity Theft on social media for the System of Banking Sector in Islamabad. *Available at SSRN 3679244*.

Schenk, S. (2008). Cyber-sexual harassment: The development of the cyber-sexual experiences' questionnaire. *McNair Scholars Journal*, *12*(1), 8.

Spitzberg, B. H., Marshall, L., & Cupach, W. R. (2001). Obsessive relational intrusion, coping, and sexual coercion victimization. *Communication Reports*, *14*, 19-30. https://doi.org/10.1080/08934210109367733

Strauss, S. L. (2013). *Sexual harassment and bullying: A guide to keeping kids safe and holding schools accountable*. Rowman & Littlefield.

Strauss, A., & Corbin, J. (1990). Basics of qualitative research: Grounded theory procedures: A model to capture the cultural and environment influences. In A. Scupola (Ed.), *Innovative Mobile Platform Developments for Electronic Services Design and Delivery*, (pp. 1-20). Hershey, PA: Business Science Reference.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics* (5th ed.). Allyn and Bacon.

Tabachnick, B. G., & Fidell, L. S. (2013). *Using Multivariate Statistics* (6th ed.). Pearson Education.

Valkenburg, P. M., Peter, J., & Schouten, A. P. (2006). Friend networking sites and their relationship to adolescents' well-being and social self-esteem. *Cyber Psychology & Behavior, 9*(5), 584-590. https://doi.org/10.1089/cpb.2006.9.584

Watkins, M. W. (2000). Monte Carlo PCA for parallel analysis, State College. PA: Ed & Psych Associates [Computer software]. Unpublished Instrument. Retrieved from https://www.softpedia.com/get/Others/Home-Education/Monte-Carlo-PCA-for-Parallel-Analysis.shtml

Willard, N. (2006). Flame Retardant: Cyberbullies Torment Their Victims 24/7: Here's How to Stop the Abuse. *School Library Journal, 52*(4), 54-59.

Ybarra, M. (2004). Linkages between depressive symptomatology and Internet harassment among young regular internet users. *Cyber Psychology & Behavior, 7*, 247-257. https://doi.org/10.1089/109493104323024500

Received 11 June 2023

Revision received 17 April 2024