Cyber Harassment and Digital Dilemma in Higher Education Institutions of Pakistan: Policy and Procedures of HEC Pakistan

Abdul Karim Kondhar[1], Irfan Ali Mallah[2], Ajaz Shaheen[3] and Ali Murtaza Shah[4]

Abstract

The study explored the cyber harassment cases in different regions, the perception of victims, and the public perspective on cyber harassment and digital dilemmas in higher education institutions in Pakistan. Furthermore, study analyzed the policy and procedures of cyber harassment cases & punishment in higher education institutions. The study was conducted through qualitative methods, and a narrative design was used. Data was collected through dual modes, document analysis & interview protocol. Initially, data was collected through related documents such as newspapers, reports, records, media reports, and government reports, and finally, data was collected through interviews with five teachers of higher education institutions in Pakistan and ten female students of higher education institutions of Pakistan with secure, shared consent and guarantee of privacy and protection about identity and data of the participants. The study explored increasing cyber harassment cases in higher education institutions and social insecurity due to digital dilemmas, which have created frustration and depression among parents, teachers, students, and stakeholders regarding cyber threats and virtual crimes against teachers and students, especially in the context of female teachers and students. Furthermore, the study explored that policy, procedures, and laws & punishment for cyber harassment believed to be so-called only in written formalities, which are null and void in implication. Cyber culprits are very intelligent to give any clue to the cyber harassment control team, and most of the time, cyber harassment culprits escape punishment, and day-to-day increasing cases of cyber harassment cases seem to be visible gaps and failures in the implementation of cyber harassment policy and procedure in higher education institutions of Pakistan.

Keywords: Cyber Harassment, Digital Dilemma, Policy & Procedures.

Introduction

Technology is an excellent source of information, a broad knowledge-sharing corridor, and a sound source of connectivity across the globe. Initially, it was confined to multinational organizations and standardized institutes of education, security, and business marketing-oriented organizations. Technology was used for formal operations such as security agencies and exploration of resources. It was almost expensive for the personal use of individuals and joint institutes. After the advance and familiarization of technology, technology access was made standard for public service to ease

[1]*School Education & Literacy Department, Government of Sindh.*
[2]*Ghulam Rabani Agro, Government Degree College Kandiaro, College Education Department, Government of Sindh.*
[3]*Faculty of Education, Lasbela University of Agriculture, Water & Marine Sciences, Uthal, Balochistan.*
[4]*Faculty of Education, Lasbela University of Agriculture, Water & Marine Sciences Uthal, Balochistan.*
Email: alimurtazashah91@gmail.com.

daily life operations (Kaputa et al., 2022). It was generally used in computer-oriented functions such as record maintenance, database, programming, entertainment, communication calculation, research & development, and social connectivity. Technology is the best mode of connectivity and communication at the cheapest rate. It provides unlimited access to execute operations such as teaching, learning, blogging, and communicating and extends the business network (Alotaibi & Mukred, 2022). It provides comprehensive access to unlimited resources for teaching and learning and facilitates innovative trends and techniques not only in education but all departments of society, It provides database and filing for the security of records, targets customers, and locates the markets of goods and services at the unlimited jurisdictions. Technology facilitated for education (teaching-learning) purposes to voluntarily ease access to faculty members, employees, students, and customers (Stevens, 2021). Institutional, more comprehensive access to technology to the public was intensively misused and violated the cyber norms and standard operating procedures of technology.

Technology has connected people and enhanced human interaction through applications of social media. Nowadays, people excessively use social media as meeting and dating sights, which has widely created abuses for the public and institutions. Internet users worldwide are advanced at an extreme inclination, and the majority use social media through mobile phones and computers to connect instantly through WhatsApp, Facebook, Twitter, Instagram, Skype, and Messenger. Technology enables individuals to connect asynchronously, through geographical boundaries, publicly or anonymously. There are a number of studies exploring that cyber harassment is being erupted as a professional crime that misleads the information, privacy, and protection of users. It has become a grave threat to the public's ability to preserve data and remain connected (Winkelman, 2015). According to Herring (1999) a perceived cyber threat is an expanding danger to break the privacy and protection of public users due to less secure connectivity and communication; most of the culprit users intend to breach personal accounts and IDs to accomplish wrong motives. It has become a common fright for users due to unlimited and insecure access to users at extreme levels, which might devastate the utilization of technology that has broken and violated the cyber ethics and users' policies and procedures (Imran, 2023).

Related Literature

Advancement of technology broadly reforms and modernizes all the fields of life, such as education, business, entertainment, marketing, banking, and communication. It inclines the ease for the user to accomplish the objective of connectivity and privacy. Technology has facilitated the human and provides multiple tasks simultaneously with accuracy and authenticity (Ali et al., 2023). Unfortunately, users manipulated the ultimate aim of technology and communication and began to use them for violence, robbing, stealing, and snatching user data and privacy. It is considered that technology has contributed to partner violence and enables perpetrators with convenient tools to intimidate, isolate, and stalk their victims through a variety of ways to destroy the norms, ethics, and use of technology (Bowen, 2012).

Hackworth (2018) explored through the study that digital media has provided space for the user to contact, interact, and share information widely. Most of the time, users are afraid of cyber phobia and digital fear of their personal information and belongings, which may cause social and cultural defame and digital disrespect to users. Users misuse information and belongings such as videos, photos, and information on social media. People consistently share and upload it on colonial digital sights, making it popular and widely accessible to several users so that they may get monetary benefits by enhancing followers, likes, comments, and watch time hours. Digital technology has

transcribed a hierarchy of penalties and charges for violation of digital information, privacy, and protection of users and authors. Cyber harassment has increased mainly due to the advent of technology and broader and easier access to the internet through digital interactions such as Facebook, WhatsApp, Viber, Instagram, Twitter, etc. (Safavi & Shukur, 2014).

Digital users have started diverse ways of harassment online, such as virtual threats, hacking devices, stealing information, accounts, and relevant data, making hidden photographs, videos, and information, and terrorizing people to seek illegal motives through cyber terrorism. Women are the greatest victims of such digital criticism, disrespect, and defaming of those famous in the region. Most of the time, cyber criminals and activists target those stakeholders who raise issues of feminism and sexism. Cyber harassment has targeted women in particular and men generally through women's gendered insults, physique critiques, and belief objections (Hussain et al., 2023). Users target sexual threats and blackmailing content for male and female genders generally. Most of the women receive attacks through misogynist and sexual terrorism through editing the photos and videos, which leads to physical torture and suicide of individual. Harassment in educational institutions has been increasing day to day with faster speed and bullying the victims and peers online (Espelage, 2019).

Technology user have created a modern mode of harassment known as cyber harassment, where they eloquently use technology to misuse individual information such as photos, videos, accounts, and intellectual property and get their interests (Fekkes et al., 2005). Cyber harassment is humiliating and threatening action with aggressive behavior (Juvonen & Graham, 2001). The digital dilemma is the contemporary challenge for the virtual user of technology where the user feels technological phobia and insecure about sharing personal resources on digital media. Cyber management procedures and policies are functional and imposed for the users of technology despite the fact that virtual fraud and cyber violence are increasing day by day worldwide. Cyber harassment affects predominantly the user of technology, such as mental sickness, isolation, insecurity, and psychological harm (Bowen, 2012). Students of universities and colleges excessively use technology; therefore, most girls are victims of cyber harassment and face cyber threats of digital sexual contact (Beran & Li, 2005). Unlike cyberbullying, cyber harassment widely hits children and teenagers and thrusts cyber misconduct and digital violation, which lead to different abuses such as rap, fraud, and kidnapping of boys and girls from educational institutions (Campbell, 2005).

The cybercrime department and digital accountability team have developed norms, ethics, and policy frameworks, developed a network of cyber security for the user of digital technology, and strived hard to control cybercrime and cyber threats for the user. Furthermore, cyber security forces the administration of educational institutions to implement policies, norms, and laws for the employees and students of the institutions so that they may secure the user incorporate cyber control in the institutions, and prevent harassment and digital dilemmas in the educational institutions (Forde & Kennedy, 1997). According to Winkelman (2015) the cyber harassment has identified the following: computer or telecommunication harassment is common for the users of technology,

1. Monitoring & hacking the email & personal data
2. Threatens e-mails, messages, and communication
3. Disrupting e-mail through the entrance in the e-mail box
4. Sending a virus program to destroy data
5. Snatching the identity of the user and sending fake messages
6. Using other information for harassment

7. Email sent through a third-party
8. Spam e-mail
9. Instant Messaging or texting
10. Posting inappropriate photos, videos & messages
11. Stalking behaviors in chatrooms
12. Blocking e-mail, Facebook, WhatsApp, and Messenger IDs
13. Hack/steal personal data and manipulate the information (photos, videos, messages, intellectual property & bank accounts)

Research Objectives

1. To explore cyber harassment in higher education institutions in Pakistan.
2. To analyze policy and procedures of cyber harassment & digital dilemmas in higher education institutions in Pakistan.

Research Questions

1. What is cyber harassment & digital dilemma in higher education institutions of Pakistan?
2. What are policies and procedures for cyber harassment & digital dilemmas in higher education institutions in Pakistan?

Research Methodology

The study examined "Cyber Harassment and Digital Dilemma in Higher Education Institutions of Pakistan: Policy and Procedures of the Higher Education Commission of Pakistan" using a qualitative methodology, explicitly applying a narrative research design. The study employed convenience sampling to collect data from two primary sources: document analysis and interviews with selected participants. The first stage entailed thoroughly analyzing various documents, such as newspapers, reports on cyber harassment, past research, media reports, and pertinent departmental documents.

The document analysis phase played a crucial role in comprehending the current state of cyber harassment in higher education institutions. Subsequently, interviews were carried out with a sample of five teachers and ten female students from several higher educational institutions in Pakistan. Individuals were selected for participation using a convenience sample procedure, and their agreement was obtained.

The specified narrative research style is appropriate for thoroughly investigating the complex issues of "Cyber Harassment & Digital Dilemma in Higher Education Institutions of Pakistan." This design comprehensively comprehends teachers' and pupils' experiences and viewpoints. The study seeks to reveal detailed accounts of cyber harassment using qualitative research methodologies, namely document analysis and interviews. This approach provides an essential understanding of the issue's complexities. The narrative research design allows for a comprehensive analysis of the subject matter, in line with the intricate and profound nature of comprehending the policy and procedural answers specified by the Higher Education Commission of Pakistan.

Study Findings

Pakistan is a democratic Islamic state in which Islamic principles and standards are intended to be enforced for both genders, particularly for women in settings where they sit together, such as educational institutions, banks, educational institutions, public and private sector institutions, and

commercial institutions. The Higher Education Commission of Pakistan has developed plans and policies in response to the issue of cyber harassment and the digital problem within educational institutions. Despite the existence of a harassment policy and system, the number of harassment incidents that occur in Pakistan's higher education institutions continues to rise daily. The vast majority of participants had the impression that the institution needed help clarifying its policies and how it governs the behavior of the masses using a variety of control measures.

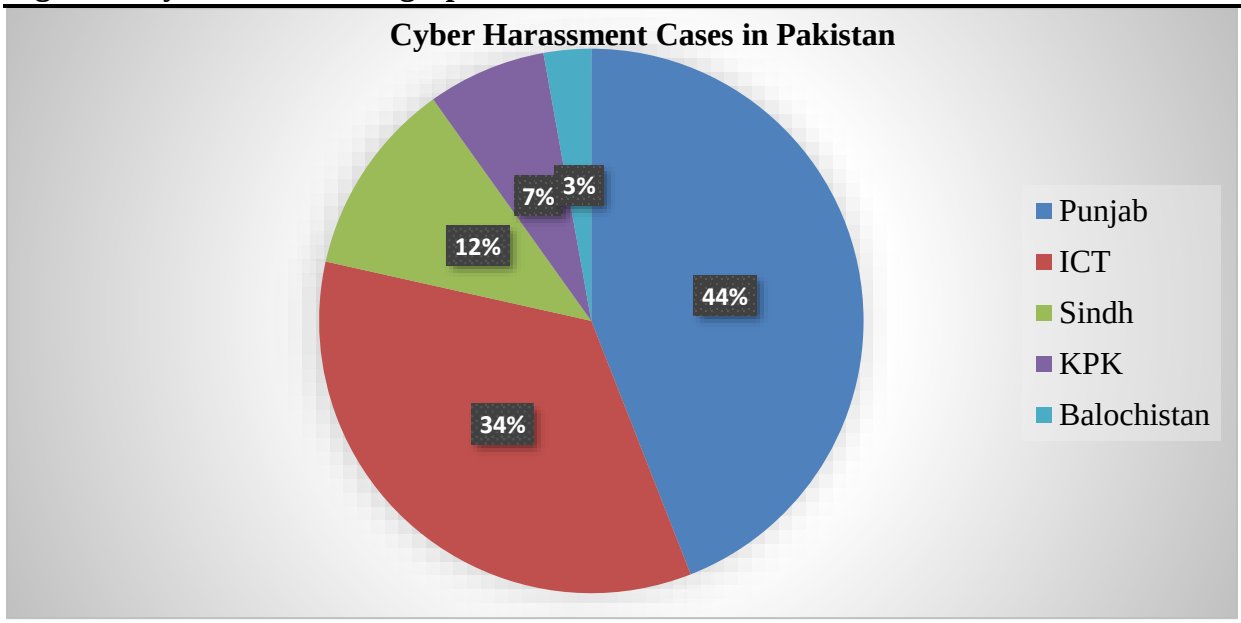
The information was obtained from various documents, including newspapers like Dawn, The News, and Jung magazines. Both the FIA and the PTA have documented the number of instances of cyber harassment in educational institutions in all four provinces. These instances are diverse in number. The number of distinct occurrences of harassment that have occurred in Pakistani areas such as Punjab, Sindh, KPK, Balochistan, and the capital region of Islamabad, which is called ICT. Findings also display the number of cases of cyber harassment that have been resolved and those that are still outstanding. Moreover, the findings shed insight into instances of suicidal behavior that have occurred across higher education institutions since 2019.

Table 1: Cyber harassment cases statistic

Total cases	**Cases of HEI**	**Suicidal Cases**			
Cyber Crime Dept. 20741	16981 (82%)	13			
FIA & PTA 5600	23716				
Federal Ombudsman (2019)	Punjab	ICT	Sindh	KPK	Baluchistan
1140	500	391	132	80	32
Resolved 1063					

The study's findings showed that the number of cases of cyber harassment in higher education institutions is growing, even though there is a policy and a mechanism to prevent it. This has become a severe problem for the government, particularly the Financial Institutions Authority (FIA), the Public Trust Agency (PTA), and cyber control agencies, as well as the administration of the institution, which is responsible for maintaining a safe and secure environment for students and teachers, particularly for female students. Other industries, such as banks, public and private schools, retail centers, markets, government offices, and non-governmental organizations (NGOs), are also experiencing an increase in the number of occurrences of cyber harassment.

Figure 1: Cyber harassment graphical overview



The participants perceived that Pakistani higher education institutions have developed policies and mechanisms to control cyber harassment and digital dilemmas among students attending higher education institutions. These policies and tools include the harassment policy, the sexual harassment policy, the sexual misconduct policy, the acceptable use and network security policy, the responsible use policy, the discrimination and harassment policy, the violence policy, the social media policy, and the student code of conduct policy. Both current regulations and their application to cyber-harassment have been the subject of inquiry committees that institutions have created.

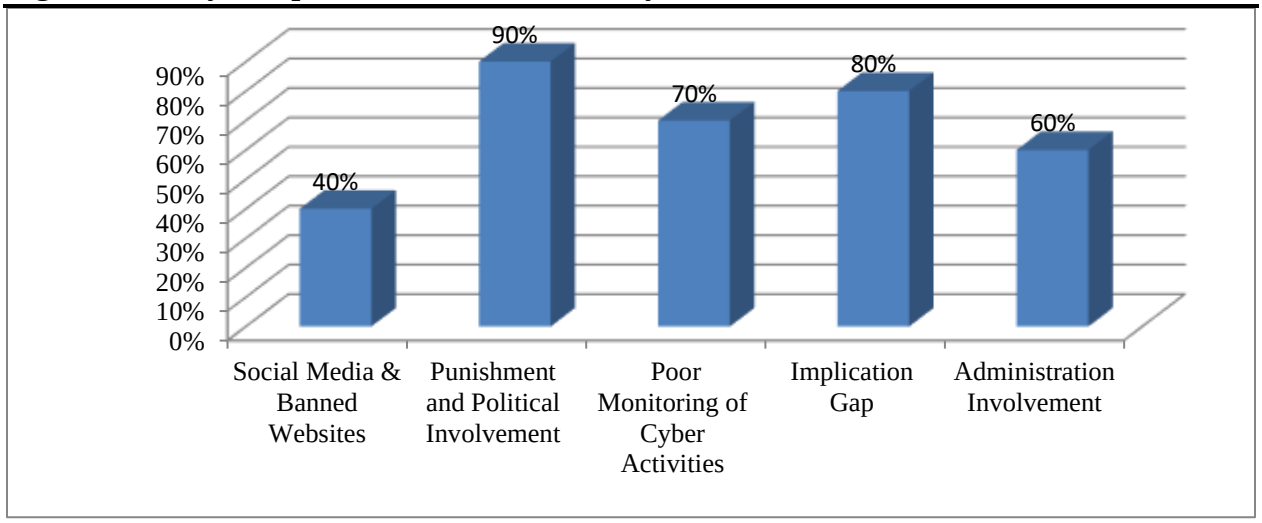
A significant number of the participants held the belief that cyber harassment is defined as the sending of unsolicited or unwanted messages, images, videos, and information from individuals who are either identifiable or unnamed, in which the girl in particular and females, in general, are subjected to comments that are threatening or undesirable. The participants thought that male students and teachers who were morally corrupt used technology to publish indecent images, videos, or other things that would be considered inappropriate and harassed female students.

Many participants thought they believed that the institution did not possess a particular policy for dealing with cyber-harassment and digital dilemmas to safeguard young women from being victimized. Participants were asked to express their definitions of cyber-harassment, and (b) institutions should rigidly implement policies and procedures on cyber-harassment. Most participants thought the institution had no predetermined policy on digital dilemmas and cyber harassment. Furthermore, the majority of the participants believed that cyber-harassment behavior ought to be dealt with within the context of the institutions by the rules now in place for cyber-harassment and digital issues.

In educational institutions, respondents believed that there needed to be a training course that could be completed online for sexual misconduct and digital misbehavior with girls. A few participants suggested that the university organize programs and sessions to raise awareness about the trends of cyber harassment and digital misconduct committed by individuals of both genders. Furthermore, participants thought that educational institutions ought to organize advice and counseling seminars to educate skills for self-realization, self-control, and self-management to

combat the cyber problem that is becoming increasingly prevalent in educational institutions. Some of the participants thought that training and lively practice should be implemented to combat cyber harassment and that women should be encouraged to develop tactics to combat harassment and protect themselves from being harassed online. Students need access to cyber assistance and counseling to combat the harassment they are experiencing.

Figure 2: Policy and procedure to control the cyber harassment



Nearly all of the participants thought that the majority of girls who drop out of higher education institutions (universities and colleges) do so in Balochistan and Sindh as a result of harassment incidents. In turn, they prevent their children from pursuing higher education. Regarding the issue of cyber harassment and digital insecurity, parents are highly dissatisfied. The growing number of instances of cyber harassment harmed the institution's reputation, which in turn posed a threat to the educational leadership and professors working in higher education institutions. Students experience feelings of digital phobia and cyber insecurity. A small number of female students have taken their own lives as a result of online harassment, and a significant number of female students have dropped out of school as a result of this predicament.

The majority of participants believed that the institution ought to have a policy that is blank-white for digital harassment and cyber misconduct and that this policy ought to be officially disseminated to all of the departments, campuses, and affiliated institutions of the educational institution. In addition, the policy and agenda, as well as the procedure for punishing digital harassment, should be pasted on every notice of each department and affiliated institution so that individuals can be aware of the code of conduct and the punishments for digital harassment. Many participants believed that the Higher Education Commission of Pakistan had devised a policy and an appropriate system to combat cyber harassment and digital dilemmas, even though it could not put these policies into exercise and put them into operation.

Cases of harassment are reported in higher education institutions all over Pakistan, according to the majority of the participants, even though there is a defined policy and framework regarding digital harassment. Most participants believed that the institution should prohibit using illegal websites and harassing digital movies, images, and websites. For academic and instructional manifestations, the supplied network services should be restricted. In addition, the Department of Student Affairs and the advisory committee regularly visit the areas where students are located

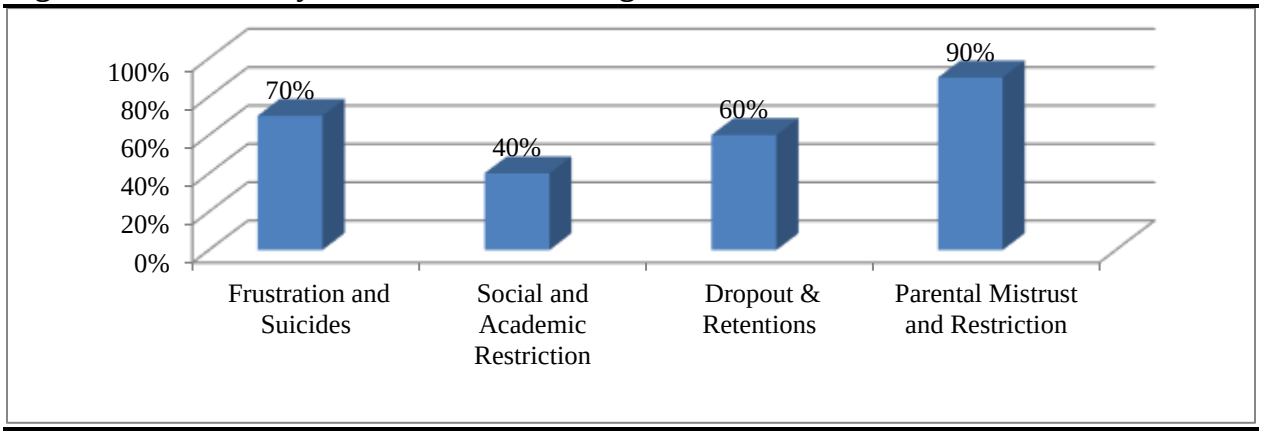
and inspect their electronic devices to safeguard and avoid inappropriate behavior in the digital realm within the educational institution. In addition, the institution ought to tightly enforce mechanisms that prohibit unlawful snaps and photographs during events and celebrations. Additionally, officials of the institution ought to be accountable for recording films and pictures, and those officials should be subjected to stringent audits and held responsible for digital crimes if the public discovers the information.

A large number of participants believed that the government of Pakistan ought to take the harassment policy and mechanism seriously, as well as demonstrate a genuine commitment to implementing digital misconduct and cyber dilemmas to provide female students with a sense of social and moral security.

Most participants thought that the harassment committee, the cyber security team, and the policy and procedure for cyber harassment are operationally ineffective and practically unimplemented. In addition, those responsible for cyber harassment are not held accountable for their actions because neither the policy nor the legislation adequately addresses the issue. When implementing strict guidelines and laws surrounding cybercrime and harassment, the Higher Education Commission of Pakistan is not as severe as it should be. As a result of the fact that cyberbullying causes frustration among parents, stakeholders, and students concerning higher education institutions, the Higher Education Commission (HEC) needs to pay strict accountability to higher education institutions about cyberbullying.

Because female students are subjected to cyber harassment and digital threats from classmates and coworkers, the majority of participants believed that the majority of parents do not allow their daughters to seek higher education. The participants felt that non-academic staff and professors should be restricted from using cameras to interact with supervisors and students. Higher education institutions in Pakistan have sought advice and services from the cyber-crime department and digital security to control digital phobia and insecurity among students, teaching staff, and non-teaching staff. Additionally, the majority of these institutions have established an Information Technology Wing and a Harassment Committee to monitor and investigate cases and issues that are related to cyber tension among users.

Figure 3: Results of cyber harassment and digital dilemma



Discussion of the Study

The study's findings provide insight into the intricate terrain of cyber harassment and digital predicaments within higher education institutions in Pakistan. Although the Higher Education Commission has implemented policies and systems, instances of cyber harassment persist, particularly impacting female students. The panelists emphasized the necessity for more explicit policies, efficient governance, and enhanced control methods to tackle the escalating difficulties (Hackworth, 2018).

The study utilized various sources, such as media records from the Federal Investigation Agency (FIA) and the Pakistan Telecommunication Authority (PTA), to evaluate the extent of cyber harassment in different provinces. These instances were diverse, and the findings emphasized promptly settling pending cases. Furthermore, the study illuminated cases of suicide behavior associated with cyber harassment, underscoring the grave repercussions experienced by victims (Stevens, 2021).

Kaputa et al. (2022) also supported that, notwithstanding the current policies, the survey unveiled a troubling surge in instances of online harassment, presenting a significant obstacle for government organizations, educational institutions, and regulatory authorities. Participants emphasized the necessity of adopting a comprehensive approach, which includes the financial institutions authority, public trust agency, and cyber control authorities, to guarantee a safe and secure environment, particularly for female students.

The study revealed various policies and strategies higher education institutions employ to address cyber harassment. Nevertheless, the participants emphasized the need for a dedicated strategy dealing with digital challenges, especially protecting female students. The study revealed that most participants believed the institution had no specific policy to address cyber harassment and digital challenges (Ali et al., 2023).

Regarding prevention and awareness, participants proposed the implementation of online training courses addressing sexual misconduct and digital misbehavior, as well as awareness programs and counseling seminars. The study highlighted the importance of providing individuals with the skills needed to achieve self-actualization and effectively govern themselves to address the growing problem of cyber harassment (Kizza, 2023).

Santre and Pumpaibool (2022) also found in their study that the repercussions of cyber harassment were substantial, as indicated by participants who observed a considerable dropout rate among female students, particularly in Balochistan and Sindh, due to harassment incidents. This ripple

effect was that parents were unsatisfied and reluctant to permit their children to seek further education.

Participants voiced discontent over the operational efficiency of the harassment committee, cyber security team, and policies on cyber harassment. Enhancing the enforcement of laws and rules, ensuring accountability, and fostering government commitment have been identified as crucial elements in tackling the digital security challenges encountered by higher education institutions (Uwalaka & Amadi, 2023).

The study's results emphasize the immediate requirement for thorough and efficient approaches to address cyber harassment and digital challenges at higher education institutions in Pakistan. The recommendations entail reassessing and fortifying current policies, promoting consciousness, and guaranteeing rigorous implementation to establish a more secure digital milieu for all those in the education sector.

Conclusion

Higher education institutions are currently facing a severe problem in the form of cyber harassment, which is a contemporary difficulty. Cases of cyber harassment are increasing in higher education institutions and other industries across Pakistan every day. It has resulted in a digital dilemma, frustration, depression, and insecurity among students, particularly female students attending higher education institutions in Pakistan. The Higher Education Commission of Pakistan develops cyber harassment policies and procedures with the consensus of the cybercrime team. Additionally, the cyber harassment and physical harassment inquiry committee has been established in every higher education institution.

Furthermore, institutions have restricted access to social media applications such as YouTube, Facebook, and WhatsApp, even though the number of cases of cyber harassment is rapidly increasing daily. It has been discovered that there is a gap in the execution of policies and procedures regarding cyber harassment and a delay in doing so. The Higher Education Commission of Pakistan has warned institutions, urging them to curb cyber and physical harassment by conducting thorough investigations into those cases and imposing severe punishments on those responsible.

References

- Ali, Z., Ahmad, N., Rehman, H. U., Ullah, N., & Zahra, T. (2023). Investigating Teacher Educators' Perceptions on Technology Integration in Teacher Preparation Programs. *Journal of Social Sciences Review*, *3*(2), 341-355. https://doi.org/10.54183/jssr.v3i2.272
- Alotaibi, N. B., & Mukred, M. (2022). Factors affecting the cyber violence behavior among Saudi youth and its relation with the suiciding: A descriptive study on university students in Riyadh city of KSA. *Technology in Society*, *68*, 101863.
- 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.
- Bowen. W. G., (2012). *Higher Education in the Digital Age*. Princeton Publishers, London.
- Campbell, M. (2005). Cyber Bullying: An Old Problem in a New Guise? *Australian Journal of Guidance and Counselling. 15*. 10.1375/ajgc.15.1.68.
- Clarke, M. (2015). The digital dilemma: preservation and the digital archaeological record. *Advances in Archaeological Practice*, *3*(4), 313-330.
- Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015). Social media update 2014. *Pew research center*, *19*, 1-2.

- Espelage, D. L., & Swearer, S. M. (2003). Research on school bullying and victimization: What have we learned and where do we go from here?. *School psychology review*, *32*(3), 365-383.
- Espelage, D. L., Valido, A., Hatchel, T., Ingram, K. M., Huang, Y., & Torgal, C. (2019). A literature review of protective factors associated with homophobic bullying and its consequences among children & adolescents. *Aggression and violent behavior*, *45*, 98-110.
- Fekkes, M., Pijpers, F. I., & Vanhorick, V. S. P. (2005). Bullying: Who does what, when and where? Involvement of children, teachers and parents in bullying behavior. *Health education research*, *20*(1), 81-91.
- Forde, D. R., & Kennedy, L. W. (1997). Risky lifestyles, routine activities, and the general theory of crime. *Just. Q.*, *14*, 265.
- Juvonen, J. E., & Graham, S. E. (2001). *Peer harassment in school: The plight of the vulnerable and victimized*. The Guilford Press.
- Hackworth, L. (2018). Limitations of "just gender": The need for an intersectional reframing of online harassment discourse and research. In *Mediating misogyny* (pp. 51-70). Palgrave Macmillan, Cham.
- Herring, S. C. (1999). The rhetorical dynamics of gender harassment on-line. *The information society*, *15*(3), 151-167.
- Hussain, A., Jat, Z. G., Hassan, M., Hafeez, A., Iqbal, S., & Imran, M. (2022). Curriculum Reforms In School Education Sector In Sindh; What Has Changed?. Journal of Positive School Psychology, 6(9), 2675-2687.
- Imran, A. (2023). Why addressing digital inequality should be a priority. *Electronic journal of information sstems in developing countries. 89*(3).
- Imran, M., Kazmi, H. H., Rauf, M. B., Hafeez, A., Iqbal, S., & Solangi, S. U. R. (2022). Internationalization Education Leadership of Public Universities of Karachi. *Journal of Positive School Psychology*, *6*(11), 1175-1188.
- Jennings, W. G., Piquero, A. R., & Reingle, J. M. (2012). On the overlap between victimization and offending: A review of the literature. *Aggression and violent behavior*, *17*(1), 16-26.
- Juvonen, J. E., & Graham, S. E. (2001). *Peer harassment in school: The plight of the vulnerable and victimized*. The Guilford Press.
- Kaputa, V., Loučanová, E., & Tejerina-Gaite, F. A. (2022). Digital transformation in higher education institutions as a driver of social oriented innovations. *Social innovation in higher education*, *61*, 81-85.
- Kizza, J. M. (2023). Cyberbullying, Cyberstalking and Cyber Harassment. In Ethical and Secure Computing: A Concise Module (pp. 199-210). Cham: Springer International Publishing.
- Lichty, L. F., & Campbell, R. (2012). Targets and witnesses: Middle school students' sexual harassment experiences. *The Journal of Early Adolescence*, *32*(3), 414-430.
- Morahan-Martin, J. (2005). Internet abuse: Addiction? disorder? symptom? alternative explanations?. *Social Science Computer Review*, *23*(1), 39-48.
- Safavi, S., & Shukur, Z. (2014). Conceptual privacy framework for health information on wearable device. *PloS one*, *9*(12), e114306. https://doi.org/10.1371/journal.pone.0114306
- Santre, S., & Pumpaibool, T. (2022). Effects of blended learning program for cyber sexual harassment prevention among female high school students in Bangkok, Thailand. International journal of environmental research and public health, 19(13), 8209.
- Shinan-Altman, S., & Cohen, M. (2009). Nursing aides' attitudes to elder abuse in nursing homes: The effect of work stressors and burnout. *The Gerontologist*, *49*(5), 674-684.

- Stevens, F., Nurse, J. R., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367-376.
- Wick, S. E., Nagoshi, C., Basham, R., Jordan, C., Kim, Y. K., Nguyen, A. P., & Lehmann, P. (2017). Patterns of Cyber Harassment and Perpetration among College Students in the United States: A Test of Routine Activities Theory. *International Journal of Cyber Criminology*, *11*(1).
- Winkelman, B. S., Oomen-Early, J., Walker, A. D., Chu, L., & Yick-Flanagan, A. (2015). Exploring cyber harassment among women who use social media. *Universal journal of public health*, *3*(5), 194.
- Winkelman, J. (2015). Insomnia Disorder. *The New England journal of medicine. 373*. 1437-1444. 10.1056/NEJMcp1412740.
- Uwalaka, T., & Amadi, F. (2023). Beyond "online notice-me": Analysing online harassment experiences of journalists in Nigeria. Journalism Studies, 24(15), 1937-1956.
- Vakhitova, Z. I., & Reynald, D. M. (2014). Australian Internet Users and Guardianship against Cyber Abuse: An Empirical Analysis. *International Journal of Cyber Criminology*, *8*(2).