POSITION PAPER

Cyber Bullying in Pakistan: The Silent Menace

'An ounce of prevention is worth a pound of cure'

DR. SYED KALEEM IMAM

04 JULY 2024

CGR

CENTRE for **GOVERNANCE RESEARCH**
PAKISTAN

ABOUT THE CENTRE FOR GOVERNANCE RESEARCH (CGR)

CGR is a forum for studies and debate on strategic and tactical issues related with good governance and the rule of law. It is a non-governmental civil society advocacy Centre dedicated to reforms in the justice and governance sectors.

As an independent think tank, CGR sets its own agenda, publishing and disseminating its findings regularly for national and global audience. Using an interdisciplinary approach, CGR brings together rule of law, justice and governance experts, researchers and internationally renowned professionals to animate its debate and research activities.

CGR aims to stand out as one of rare Pakistani think tanks to position itself at the very heart of debate on governance and justice issues.

CGR focuses on advocacy, research and studies in the following areas:

- Governance and Rule of Law
- Public Policy
- Policing and Justice Sectors
- Serious and Organized Crimes
- Counterterrorism and Counter Extremism (CT and CE)

Meanwhile, the National Initiative against Organized Crime (NIOC) continues as a flagship project from the platform of the Centre for Governance Research (CGR).

***

ACKNOWLEDGMENT

CGR would like to acknowledge that this position paper has been written by Dr Syed Kaleem Imam, former Inspector General of Police and Federal Secretary Narcotics Division.

Position Paper

Cyber Bullying in Pakistan: The Silent Menace

'An ounce of prevention is worth a pound of cure'

BY
DR. SYED KALEEM IMAM

Introduction

In the age of virtual reality, where the world seems just a tap away, we now face a growing issue - cyberbullying. This development infiltrates the online domain through harassment and intimidation tactics on various online forums such as social media, instant messages, electronic mails, and other grids. It is more than just an inoffensive internet prank; it is insidious, transcending physical boundaries unlike traditional harassment, and invading victim's cybernetic space (PACER, 2022).

However, cyberbullying is distinguished by its anonymity, as perpetrators mask identities to intimidate victims with impunity. The tactics employed by a cyberbully are extensive and perilous, ranging from impersonation and cyberstalking to phishing (disclosing personal credentials by clicking on hostile links), trolling (sarcasm, insults), and outing (revealing personal information non-consensually). These web assaults, whether through abusive and insolent remarks or data leakage, imprint psychological wounds on victims.

Cyberbullying has become a global challenge, with countries like India and Brazil reporting high prevalence. Around 37% of internet users in India and 29% in Brazil have reported being cyberbullied (Cook, 2024). Pakistan, not exempt, has witnessed a surge in internet penetration and social media use, with 76.38 million online users (Bhatti, 2022). The increase in internet consumption has corresponded with a rise in cyberbullying cases. A 2019 study by Digital Rights Foundation (DRF) illustrates that Pakistan has reported 45% of cyberbullying cases (Jamal, 2020). Thus, online intimidation has emerged as a serious peril to online society's well-being.

Cyberbullying in Pakistan

Evolution and Trends

In Asia, Pakistan has one of the largest mobile phone user bases. National Cyber Crimes Investigation Agency (NCCIA) has recently replaced the Federal Investigation Agency (FIA) as head of internet guidelines in Pakistan, which is governed by the Pakistan Telecommunication Authority (PTA). Data compiled by these authorities shows contentious measures among internet users, ranging from data breaches, propaganda, and the marginalization of religious and gender minorities. According to the Global Cybersecurity Index (GCI), released by the International Telecommunication Index in 2020, Pakistan ranks 79th in cybersecurity, highlighting the country's engagement in cybers protection among the signatories.

In 2020, FIA's cybercrime department lodged over 85,000 complaints, primarily concerning investment scams, counterfeit profiles, credential theft, false accusations, bigotry, cyber shakedown, and cyber blackmail. According to the Digital Rights Foundation (DRF), over 146 monthly calls have been reported by their cyber harassment helpline, with 57% of the objections raised by women and 30% by men. Punjab constitutes 57% of the documented instances, followed by Sindh with 15% (The Nation, 2023).

The most alarming aspect of the DRF's review is the demographic segment between 21 and 25, with mostly victims in the youth segment. The increase in online stalking cases coincided with the onset of coronavirus pandemic and improvement in digital inclusion. Individuals who experienced internet trolling were therefore 1.9 times more likely to consider suicide.

Almost 90% of Pakistani university students have also reported cyber bullying, with affluent classes being more exposed (Ibid). Moreover, the impact of digital abuse on women's well-being, especially female journalists, is unsettling. Figures reveal that 9 out of 10 female journalists in Pakistan have been exploited by internet bullying, and 40% of the female demographic has been exposed to it.

Child pornography is used as a weapon to intimidate or manipulate juvenile victims escalating their victimization and exploitation. From 2021 to 2023, through an in-depth analysis of cyberbullying instances in Pakistan, out of 464 documented cases, only 184 were formally recorded. This contained 312 local complaints, 150 via CyberTipline, and 2 from external referrals, signaling potentially rigorous registration requirements or screening mechanisms within the legal protocol.

While 225 arrests were conducted from the 184 reported incidents, the below-average conviction rate of only 23 rulings reinforces the significant barriers in procuring satisfactory evidence for effective prosecutions in

pornography cases. Furthermore, the acquittal ratio of 31 compared to convictions underline the dilemmas in proving cyberbullying charges and handling online evidence. From 2021 to 2023, out of a total of 134,669 registered complaints, approximately 80.7% were from males, while approximately 19.3% were from females. Only 4 complaints were reported from transgender individuals.

From 2018 to early 2024, female harassment claims under the Prevention of Electronic Crimes Act (PECA) Act 2016 marked a significant increase, rising from 310 in 2018 and peaked to 11,723 in 2023. However, out of a total of 27,867 complaints during this period, only 1,717 cases were registered, indicating a low registration rate of approximately 6.2%. Similarly, while 1,689 arrests were made, only 67 convictions were secured, reflecting a low conviction rate of roughly 0.24% relative to the total complaints and about 3.9% relative to the registered cases.

The latest data for 2024 depicted a notable decline in all categories, with only 59 cases registered and 48 arrests made from 1,854 complaints, and just 4 convictions. This suggests inconsistent enforcement and underreporting or simply partial year data.

District wise, the Islamabad Cyber Crime Reporting Center accumulated 20,527 reports, with 10,449 in 2022 and 10,078 in 2023. In the Hazara division of KP province, the Cyber Crime Reporting Center in Abbottabad received a total of 3,921 cybercrime claims, with 1,997 in 2022 and 1,924 in 2023. The complaint volume, a total of 12,666, was highest in Peshawar.

In Punjab, the Cyber Crime Reporting Centers observed major activity particularly in Lahore which had the maximum complaints with a total of 33,729. In Sindh, the Hyderabad division registered the most complaints with a total of 6,205. In Balochistan, Quetta division experienced maximum complaints with 2,854. In Gilgit-Baltistan, the Gilgit division recorded 1,222 complaints, leading in the region. Azad Jammu and Kashmir saw a notable trend, with Mirpur and Muzaffarabad divisions reporting 985 and 681 complaints, respectively.

Collectively, there were 249,292 cybercrime cases registered, with 140,595 in 2022 and 108,830 in 2023, highlighting a minor dip in the count of complaints over the two-year period.

Factors Contributing to Cyberbullying

Cyberbullying is an escalating challenge in Pakistan, and enforcement bodies confront various difficulties in adeptly resolving it.

Political Factors:

The legal foundation regulating cyber offense in Pakistan remains embryonic and encounters repeated amendments. While the application of PECA reflected a promising growth, critics posit that it elevates national interests over individual privileges. This contrast discourages victims from registering incidents of digital abuse due to perceived state intervention.

Cyberbullying, although a key problem, is often suppressed by more critical issues in Pakistan, such as militancy and economic fragility. The lack of political stability and polarization results in a funding deficit and resource deployment for authorities tasked with combating cybercrime. Corruption within enforcement agencies further escalates the predicament as it disrupts inquiries (Haque et al., 2023). This is exacerbated by limited resources or incentives

to pursue cases of digital victimization. Thus, lack of transparency within the framework promotes unreported cases within the society.

Economic Factors:

A significant obstacle in addressing cyberbullying in Pakistan arises from poor digital aptitude prevalent among a substantial demographic. The gap in digital literacy leads to online frauds and deception, increasing vulnerability to cyberbullying. Without appropriate insights of web safety precautions, users may have difficulty in acknowledging and reacting to cyberbullying cases positively.

Furthermore, socioeconomic factors such as frustration stemming from economic hurdles, as well as shortage of resources and infrastructure within law enforcement, delay the effective alleviation of cyber harassment. This includes scarcity of e-discovery tools and a shortage of skilled cybercrime specialists. Under-resourced security forces experience setbacks to recognize criminals and ensure accountability, further amplifying the rate of cyber aggression in the country.

Social Factors

Societal pressures breed insecurities, resulting in cyberbullying those individuals who are perceived as atypical. The absence of strong social networks, both online and in-person, leaves victims defenseless to such attacks. Likewise, a lack of familiarity about web protocols along with normalization of cyberbullying habits within certain social circles promotes a haven conducive for this notorious behavior.

These determinants create an environment where cyberbullying prospers. Without resilient statutory provisions, administrative dedication, and necessary funding, law enforcement struggles to curb and conduct cyberbullying investigations.

Impact of Cyberbullying on Families and Communities

Cyberbullying's reach spans far and wide beyond the victim, spreading anxiety within families and communities in Pakistan.

Stress on Victim

Victims of online bullying mostly suffer severe psychological distress, leading to despair, desolation, rage and humiliation. It can spark depression, anxiety, and a sense of alienation and estrangement. In extreme cases, the negativity can generate suicidal thoughts. These non-stop attacks can also undermine a victim's self-esteem, making them apprehensive of using technology and distrustful of the online world.

Effect on Family

The emotional strain of online harassment is not limited to the victim alone; it is perceivable throughout the family. Witnessing loved ones in this ordeal can leave families feeling vulnerable, infuriated, and terrified, jeopardizing family ties. Victims may become introverted and isolated, further avoiding communication within relationships.

Bearing on Community

In the wider context, cyber victimization pollutes the ambience, primarily for youth. It promotes fear and suppresses open discussions and dialogues. Internet anonymity aggravates a bystander effect, with communities unwilling to assist as they fear victimization. This spurs a culture of skepticism, where uncertainty

prevails. In some communities, victims undergo social exclusion or even held accountable, deepening their social alienation and emotional distress.

Notable Cases

Several noteworthy cases of online bullying have occurred in Pakistan. In 2016, shortly after the implementation of PECA, an assistant professor was detained for harassing a female teacher online. A teacher issued a complaint after being intimidated on social media through five fabricated profiles. This case underscored the importance of new law, safeguarding victims from online abuse. PECA includes clauses for punishment of up to one year in prison or a hefty fine for misconducts like manipulation, inappropriate distribution of private pictures and sending obscene messages (Esmezyan, 2016).

In 2020, Fatima Aamir, became a victim of digital intimidation and received rape and murder threats for four years (Bokhari, 2020). However, the culprit was finally detained following public uproar. Similarly, Bina Shah, a Pakistani author and columnist faced cyber harassment in 2014 when an individual created a fake Twitter profile with her pictures. The perpetrator, impersonating Shah, contacted people she was acquainted with, both online and in-person, and harassed them.

E-security intrusions have had fatal repercussions in Pakistan, with content fabrication being a key contributor to the problem. One renowned case involved Dr. Amir Liaquat, a prominent presenter and politician, who succumbed to suspected suicide following the leak of private videos.

Legal Framework: Addressing Cyberbullying in Pakistan

PECA, enacted by the National Assembly of Pakistan in 2016, serves as Pakistan's legal framework for approaching digital abuse and other electronic breaches. Section 21 fines online antics that harm reputation and compromises privacy, punishable by up to 7 years imprisonment or a hefty fine. Similarly, Section 22 enforces similar punishments for falsification and propagation of explicit content involving minors. Cyberbullying is recognized as a misdemeanor under PECA, with policies covering defamation, privacy infringement, and circulation of disturbing content (Ministry of Law and Justice, 2022).

Recently, PECA proposes to update the legal framework, but sustaining a symmetry between online protection and privacy rights remains challenging (Pakistan Today, 2024). While PECA provides a legal roadmap for grassroots awareness and ensuring prompt execution, enhancing web security are important next steps.

Despite efforts to address cyber harassment and advocate for freedom of speech and privacy protections, PECA is impeded by public ignorance about online security laws and digital entitlements compromising PECA's effectiveness.

PECA assigns investigative and judicial assignments for cybercrime to the Federal Investigation Agency (FIA), including felonies committed through electronic means. Court proceedings for these violations happen in Courts of Sessions and higher courts, overseen by judges who are trained in cyber insights, forensics, web transactions, and data integrity. Also, the Pakistan Telecommunication Authority (PTA) regulates telecommunications

entities and has the permission to bar illegal content.

In 2021, Pakistan made significant progress in bolstering online security with the release of its first National Cyber Security Policy. This framework aims to handle critical cyber risks nationwide and construct a digital domain for both government and private areas. The plan summarizes a blueprint for achieving milestones in internet security, including virtual governance, digital solutions, human resources, and public awareness (Government of Pakistan, 2021). The guideline prioritizes forceful cybersecurity structures and establishments. It also highlights confidentiality measures, digital privacy, and development of public understanding and skilled personnel to mitigate cyber risks.

To ensure effective enforcement, the policy implements a Cyber Governance Policy Committee. This committee encourages partnership between state, corporations, and civil society. The multidimensional strategy includes preemptive protection of online platforms, securing national data and infrastructure, and facilitating public-private cooperation. The committee also emphasizes capacity building, cybersecurity research and innovation, and broadening public awareness about cyber-attacks.

Furthermore, the Digital Rights Foundation (DRF) advocates cyber safety practices through lobbying. This NGO aims to build reliable digital policy, with a focus on women's rights in internet forums. They achieve this by supporting pertinent policies and spreading knowledge about electronic security and safeguarding women from internet harassment.

Acknowledging the universality of digital threats, the need for international cooperation is paramount. UNICEF is working to promote cyber safety awareness. Based on an international survey on youth discussions, UNICEF issued a call to action on Safer Internet Day. The poll received over 1 million responses from 160 countries. The survey showed that young people valued kindness as defense against cyberbullying. This priority on youth-driven approaches and a constructive online protection approach corresponds well with Pakistan's initiatives to collaborate with global forums.

Notwithstanding its progress, Pakistan also needs to embrace the Budapest Convention, a multilateral pact designed to combat online offenses and stimulate global partnership in fighting cyber law violations. As a pioneering pact on cybercrime, this treaty was ratified by 68 countries as of June 2024. The Convention addresses a spectrum of cybercrimes, including unauthorized infiltration into digital systems, hacking, data fraudulence, and child sexual exploitation content. It promotes cross-border alliance among participant states in investigating and litigating these breaches through joint evidence sharing and collective legal cooperation.

Pakistan's non-participation in the treaty poses significant challenges in successfully curbing international internet crimes. Without participation, PECA lacks the necessary infrastructure to deal with cyber offenders operating from foreign jurisdictions. International authorities cannot aid Pakistan in gathering evidence, locating, tracing, and intercepting cyber intrusions from other countries. This lack of global partnership limits Pakistan's potential to handle cyber breaches cases overseas.

The Convention could provide a platform for formulating improved frameworks and ordinances, augmenting forensic expertise and investigative abilities. While there are apprehensions about confidentiality and data autonomy, opting out of any international cybercrime agreement could impede Pakistan's ability to confront the escalating danger of cross-border cybercrimes and synchronize with international initiatives (Mahmood, 2022).

Keeping up with cyberbullies' evolving tactics requires continuous legal reform and policy updates. For cyberbullying to be effectively combated, PECA should be regularly reviewed and updated

Preventing Cyberbullying: Strategies and Recommendations

Here are some viable strategies for acknowledging, preventing, and responding to cyberbullying incidents:

Parental guidance: Children need open communication from their parents in order to be protected. Encourage your children to report cyberbullying incidents by engaging in transparent discussions about their online interactions, informing them about privacy settings and the dangers of sharing sensitive information online.

Schools' Protocols: A safe environment for disclosure and awareness can help schools tackle cyberbullying. The first step is to establish clear channels and protocols for reporting. Schools should help victims and perpetrators, focusing on education and rehabilitation.

Awareness Campaign: The public should be educated on cyberbullying through public awareness campaigns. Cyberbullying awareness campaigns should include workshops, social media campaigns, and collaborations with influencers to raise awareness.

Cybersecurity Education: This should be integrated into institutes programs to teach employees about safe online practices, recognizing cyberbullying, and responding to it. Anti-bullying measures can help prevent cyberbullying

For Internet Users: Constructive communication, respectful dialogue, and considerate interactions are crucial to creating a reliable online environment. Online content must be considered before it is circulated. A proactive approach is needed to address internet harassment. Informing the designated authorities of such incidents and offering assistance to the victim are essential steps. Support groups and counselling services should be established for cyberbullying victims.

Role of Tech Companies: Companies in the technology sector must play a vital role in preventing and addressing cyberbullying. Among the steps involved are implementing vigorous reporting mechanisms, incorporating artificial intelligence to detect harmful content, and promoting digital literacy among users.

Cross-Border Collaboration: Cyberbullying, which often transcends borders, requires international cooperation. International cybercrime forums and treaties, such as the Budapest Convention, should be engaged by Pakistan for cross-border collaboration

Law Enforcement: For law enforcement to effectively combat cyberbullying, they must have cybersecurity forensics, investigation skills, and legal knowledge. Schools and internet services should collaborate to create transparent reporting structures, empowering

victims and enabling bystander intervention. A variety of initiatives, such as seminars, public service announcements, and crisis lines, can aid in preventing cyberbullying. Detection and prevention of incidents are essential with online platforms.

Conclusion

Cyberbullying requires a collective effort to cultivate a secure and holistic digital landscape. This approach incorporates legal ramifications, educational endeavors, and societal support. It is not only about protecting people but building a respectful online culture where everyone can thrive. By promoting awareness, enforcing deterrent strategies for malicious behavior, and extending help to victims, we can empower digital citizenship where everyone feels safe to participate.

Bottomline: 'Together, we can turn the tide against cyberbullying and create a safer digital world for all'

References

- Bhatti, H. (2022, February 16). Cyberbullying in Pakistan: The Case of Cyber Harassment Against Women. Paradigm Shift. https://www.paradigmshift.com.pk/cyberbullying-in-pakistan/
- Bokhari, A. (2020). Silent Battles: How Pakistani Women Counter Harassment in Cyberspace. Thediplomat.com. https://thediplomat.com/2020/10/silent-battles-how-pakistani-women-counter-harassment-in-cyberspace/
- Cook, S. (2024, January 10). Cyberbullying Statistics and Facts for 2016 - 2018 | Comparitech. Comparitech; Comparitech. https://www.comparitech.com/internet-providers/cyberbullying-statistics/
- Data retrieved from FIA Cyber Crime Wing
- Esmezyan, T. (2016, January 22). How Pakistani women are fighting against online harassment. Global-Citizen.com. https://global-citizen.com/business/social-business/cyber-bullying-women-pakistan-nighat-dad/
- Government of Pakistan. (2021). National Cyber Security Policy 2021. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf
- Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber Forensic Investigation Infrastructure of Pakistan: An Analysis of the Cyber Threat Landscape and Readiness. IEEE Access, 11, 40049–40063. https://doi.org/10.1109/ACCESS.2023.3268529
- Hinduja, S., & Patchin, J. (2019). Cyberbullying: Identification, Prevention, & Response. https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2019.pdf
- Jamal, S. (2020, July 1). Cyber harassment on the rise in Pakistan, report says. Gulfnews.com. https://gulfnews.com/world/asia/pakistan/cyber-harassment-on-the-rise-in-pakistan-report-says-1.72354581
- Mahmood, F. (2022, November 21). Should Pakistan sign the Budapest Convention? The Express Tribune. https://tribune.com.pk/story/2387309/should-pakistan-sign-the-budapest-convention
- Ministry of Law and Justice. (2022). Prevention of Electronic Crimes Act, 2016. Pakistancode.gov.pk. https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-jjjjjjjjjjj
- PACER. (2022). Cyberbullying. www.pacer.org. https://www.pacer.org/bullying/info/cyberbullying/
- Pakistan Today. (2024, May 9). PM Shehbaz approves Peca law amendments to regulate social media. Pakistan Today. https://www.pakistantoday.com.pk/2024/05/09/pm-shehbaz-approves-peca-law-amendments-to-regulate-social-media/

- Saleem, S., Khan, N. F., & Zafar, S. (2021). Prevalence of cyberbullying victimization among Pakistani Youth. Technology in Society, 65, 101577. https://doi.org/10.1016/j.techsoc.2021.101577
- The Nation. (2023, September 18). Youth at risk: cyber-bullying epidemic grips Pakistan. The Nation. https://www.nation.com.pk/18-Sep-2023/youth-at-risk-cyber-bullying-epidemic-grips-pakistan
- UNICEF. (2019). Safer Internet Day: UNICEF calls for concerted action to prevent bullying and harassment of young people online in Pakistan. www.unicef.org. https://www.unicef.org/pakistan/press-releases/safer-internet-day-unicef-calls-concerted-action-prevent-bullying-and-harassment
-

ABOUT THE AUTHOR

Dr. Syed Kaleem Imam is a former civil servant, known for his extensive contributions in law enforcement, academics, and organizational development. He has a PhD in Politics and International Relations and an LLM in Human Rights Law from SOAS, UK, master's in philosophy.

He held the position of Inspector General of Police (IGP) in several regions such as Punjab, Islamabad, and Sindh, further serving twice on the National Highways and Motorways. As the Federal Secretary of the Narcotics Control Ministry, he played a key role in formulating national policies that harmonized with international strategies.

He has been the Chief of Operations in Mozambique, Planning Coordinator in Liberia, and UN Police Commissioner in Darfur, Sudan. His service was honored with three UN peace medals, the Quaid Azam Police Medal, the President's Police Medal, and the Sitara Imtiaz and Tamagha-i-Imtiaz.

Moreover, Imam has been instrumental in shaping academic discourse through his numerous national and international publications to his credit and frequently participating in public forums, training institutes, and media outlets. Besides being a security analyst, he is also a law and governance consultant, a strategist, and a policy practitioner.

CGR

CENTRE for GOVERNANCE RESEARCH
PAKISTAN

www.cgr.com.pk
CgrPakistan
CgrPakistan

Islamabad office:
#38-W, Khalid Plaza, 1st. Floor. Jinnah Ave. Blue Area. Islamabad Phones 051-2870852 & 2870853.

Lahore office:
22, Tipu Block, New Garden Town, Lahore
Phone: 042-35831352