Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January-June 2023 4(1), 1182–1187

CYBERTHREATS, CYBERBULLYING, AND CYBERSTALKING: A CRITICAL EXAMINATION OF DIGITAL HARASSMENT IN THE CONTEMPORARY ERA

Sumaira Hamid [1], Dr. Khursheed Ahmad Qazi [2]

[1] Research Scholar University of Kashmir North Campus
[2] SG Assistant Professor and Coordinator North campus University of Kashmir

DOI
10.29121/shodhkosh.v4.i1.2023.3132

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

With the rapid evolution of digital technologies, the internet and social media platforms have become integral to modern life. However, these advancements have also given rise to new forms of harassment, such as cyberthreats, cyberbullying, and cyberstalking. Each of these forms of online abuse can have far-reaching consequences on individuals, particularly regarding their mental health and safety. This paper critically examines the nature, psychological effects, and legal frameworks surrounding these forms of digital harassment. By analyzing specific real-world cases like the Bulli Bai and Sulli Deals apps, the paper emphasizes the urgency of tackling these problems through more robust legal measures, social awareness, and support systems for victims. The paper also explores preventive strategies that can be implemented by individuals, technology companies, and lawmakers to reduce the incidence of digital harassment and ensure safer online spaces.

Keywords: Cyberthreats, Cyberstalking, Cyberbullying, Harassment

1. INTRODUCTION

The internet has revolutionized communication, information sharing, and social interaction. With platforms like social media, email, and messaging apps, individuals can stay connected across the globe. However, with these advancements also come significant risks. Cyberthreats, cyberbullying, and cyberstalking are three major forms of digital harassment that have emerged as critical issues in the modern digital landscape. These problems can affect anyone—regardless of age, gender, or background—and can cause lasting psychological damage, social disruption, and, in extreme cases, even lead to self-harm or suicide. Benson and McAlacny in their book *Emerging Cyber Threats and Cognitive Vulnerabilities* (2019) writes:

> The emergence of digital technologies has seen the proliferation of new online communications, providing opportunities for increased social interaction in an accessible manner. This availability to communicate online is an embedded feature of society, particularly predominant amongst young people (Ofcom, 2016). While the internet affords many social and recreational benefits, it also offers numerous positive implications across a variety of industry sectors (Finkelhor, 2014). Despite this, the increased access to online communication can increase

vulnerability to a variety of online risks including harassment, cyberbullying and other cyberthreats on privacy or online data (Livingstone, Haddon, Görzig, & Ólafsson, 2011). Although experiences online including pornography, contact with strangers, sharing personal information, exchanging explicit personal photographs (i.e. sexting) and hacking may not lead to harm, their existence could increase the probability of harm. While experience with these cyberthreats can lead to negative experiences and adverse consequences, not all result in actual harm (Livingstone & Smith, 2014) (1-2).

The anonymity that digital platforms offer allows perpetrators to engage in harmful behaviors with reduced fear of detection or punishment. As these issues continue to grow, it becomes increasingly important to understand the nature of these digital harms, their impact on victims, and the ways in which they can be addressed both legally and socially. This paper explores these phenomena, examining their characteristics, the ways they manifest, the impact they have on individuals and society, and the ongoing legal and preventive measures needed to mitigate these risks.

1) Cyberthreats

Cyberthreats refer to potential dangers in the digital domain that can harm individuals, organizations, or systems. These threats often exploit vulnerabilities in networks, software, or hardware to gain unauthorized access to data or disrupt services. Maria Bada and Jason R. C. Nurse in their research article "The Social and Psychological Impact of Cyber-Attacks" writes:

The impact of cyberspace on society is undeniable. It has provided a platform for instantaneous communication, commerce and interaction between individuals and organizations across the globe. As cyberspace has grown in prominence however, unfortunately so too has the number and variety of cyber-attacks (Verizon, 2018). Cyberattacks are defined here as events which aim to compromise the integrity, confidentiality or availability of a system (technical or socio-technical). These attacks range from hacking and denial-of-services (DoS), to ransomware and spyware infections, and can affect everyone from the public to the critical national infrastructure of a country (Nurse, 2018).

The main types of cyberthreats include:

Phishing: This is a form of fraud where cybercriminals impersonate legitimate institutions (e.g., banks, tech companies) to trick individuals into revealing sensitive information such as passwords, social security numbers, or credit card details. Phishing attempts are often conducted via emails, social media messages, or fake websites that look like legitimate ones.

Malware: Short for "malicious software," malware is a type of program designed to disrupt, damage, or gain unauthorized access to computer systems. This includes viruses, worms, Trojans, and spyware. Malware can be delivered through email attachments, infected websites, or downloadable software.

Ransomware: Ransomware is a form of malware that locks a user's computer or encrypts their data and demands payment (often in cryptocurrency) in exchange for restoring access. Famous examples include the WannaCry and NotPetya attacks, which affected thousands of businesses and individuals worldwide.

Distributed Denial of Service (DDoS) Attacks: In a DDoS attack, attackers overload a website or server with excessive traffic, rendering it unavailable to users. DDoS attacks are often used by hackers to disrupt services for political, financial, or ideological reasons.

2. PSYCHOLOGICAL IMPACT ON VICTIMS

Cyberthreats, particularly those involving data breaches, identity theft, or financial loss, can cause severe psychological distress. Victims may experience anxiety, depression, and fear of further attacks. The breach of personal information can create feelings of violation and vulnerability, particularly when sensitive information (e.g., medical records, personal photos) is stolen. The fear of being targeted again can lead to heightened paranoia, affecting the victim's overall mental health and wellbeing. Long-term consequences can include a loss of trust in online platforms, social isolation, and financial difficulties caused by fraud or identity theft.

3. PREVENTIVE MEASURES

Preventing cyberthreats requires both individual vigilance and collective responsibility. Some key preventive measures include:

Strong Passwords: Using complex, unique passwords for each account significantly reduces the likelihood of a successful cyberattack.

Multi-Factor Authentication (MFA): Enabling MFA adds an extra layer of security to accounts by requiring more than just a password to access an account. This makes it harder for attackers to gain unauthorized access.

Regular Software Updates: Keeping operating systems and applications up-to-date ensures that known vulnerabilities are patched, reducing the chances of exploitation by cybercriminals.

Awareness and Education: Teaching individuals how to recognize phishing attempts, avoid suspicious links, and practice safe online behavior is vital in preventing cyberthreats.

2) Cyberbullying

Cyberbullying involves using the internet or other digital technologies to harass, threaten, or manipulate others. Unlike traditional bullying, which generally takes place in person, cyberbullying can occur at any time, often 24/7. The most common forms of cyberbullying include:

Harassment: Sending threatening, abusive, or offensive messages via social media, emails, or messaging platforms. This form of bullying is typically sustained over a period, with the perpetrator continuously targeting the victim.

Exclusion: Excluding someone from online activities or social groups (e.g., excluding them from a group chat or social media event). The victim may feel isolated and rejected, leading to emotional distress.

Impersonation: Creating fake profiles or hacking into accounts to impersonate someone and spread false information, rumors, or embarrassing content about the victim.

Doxing: The practice of publicly releasing private information about an individual without their consent, often with the intent to harm their reputation or endanger their safety.

4. HIGH-PROFILE CYBERBULLYING CASES

Several high-profile cases of cyberbullying have garnered attention in recent years, underscoring the serious impact this form of harassment can have on individuals. Two significant incidents in India were the Bulli Bai app and the Sulli Deals controversy.

The Bulli Bai App (2022): This app was created to auction Muslim women, often without their consent, by using their photographs taken from social media platforms. The perpetrators used derogatory and objectifying language, reducing women to mere commodities. The app's use of the term "Bulli Bai" (slang for "ugly girl") reflected the malicious intent behind the app, targeting women based on their religion and appearance. This incident shocked the public and brought attention to online misogyny, especially the use of technology to facilitate harassment and hate speech against women.

The Sulli Deals (2021): This case involved a similar incident where Muslim women's photos were taken from their social media accounts and listed in an online "auction." Although it was not an actual auction, it was meant to demean and objectify the women. Both incidents were quickly reported by media outlets, and investigations were launched to identify the perpetrators. These cases highlight the intersection of cyberbullying and religious discrimination, demonstrating how technology can amplify hate speech and target marginalized groups.

5. PSYCHOLOGICAL AND EMOTIONAL IMPACT

Cyberbullying often has severe psychological consequences. Victims may experience depression, anxiety, and a significant decline in self-esteem. The public nature of online harassment makes it particularly harmful, as it can lead to widespread humiliation. Victims may feel trapped, as they are unable to escape the harassment and may withdraw from social media platforms or even real-life social interactions. The long-term effects can include lasting emotional trauma, with some individuals reporting feelings of loneliness, hopelessness, and even suicidal ideation.

6. LEGAL FRAMEWORK

Laws regarding cyberbullying vary significantly across different countries. In India, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, aim to regulate online harassment, including cyberbullying. However, there is no specific law that directly addresses cyberbullying, which often makes it difficult to prosecute offenders. In contrast, countries like the United States and the United Kingdom have more robust legal frameworks, with specific laws criminalizing cyberbullying. Victims of cyberbullying often face challenges in proving their case, as perpetrators typically remain anonymous. This underscores the need for stronger digital regulations and mechanisms to protect individuals from online harassment.

3) Cyberstalking

Cyberstalking is analogous to traditional forms of stalking in that it incorporates persistent behaviours that instil apprehension and fear. However, with the advent of new technologies, traditional stalking has taken on entirely new forms through mediums such as email and the Internet. Thus, it becomes cyberstalking. Increasingly, cyberstalking is gaining the attention of the media and the public as the nature of the crime incorporates elements of new technology and threatening behaviours, which symbolise a new form of threat (Ogilvie 1-2).

Cyberstalking involves the repeated use of the internet or other forms of electronic communication to stalk or harass an individual. Unlike cyberbullying, which may involve multiple targets, cyberstalking typically focuses on a single individual and is characterized by persistent, often obsessive, behavior. Cyberstalkers may use various methods to monitor, intimidate, and control their victims, including:

Monitoring: Tracking the victim's activities through social media, GPS, or other online tools.

Sending Harassing Messages: The perpetrator may send repeated threatening or unwanted emails, messages, or phone calls to the victim.

Public Humiliation: Posting defamatory or embarrassing content about the victim online, often aimed at destroying their reputation.

Emma Ogilvie in her research article "Cyberstalking" writes:

> In one example, a female university lecturer was stalked for some years. Her ex-boyfriend would visit her usual chat sites, and then follow her from site to site, recording where she went. He also posted false information about her in various chat sites, including both those she habited and pornography sites that he visited. Finally, he hunted down and distributed semipornographic photographs of her as a young girl across the net (Gilbert 1999). In another example, a woman was stalked for a period of 6 months. Her harasser posted notes in a chat room that threatened to rape and kill her, and posted doctored pornographic pictures of her on the net together with personal details (Dean 2000).

7. PSYCHOLOGICAL EFFECTS ON VICTIMS

Victims of cyberstalking can experience intense fear, anxiety, and a constant sense of being watched. The emotional toll of being stalked online can lead to significant distress, causing victims to feel powerless and vulnerable. The inability to escape the harassment, due to the 24/7 nature of the internet, can exacerbate feelings of paranoia and isolation. In some cases, victims may suffer from Post-Traumatic Stress Disorder (PTSD), depression, and other long-term mental health issues.

8. LEGAL CONSIDERATIONS AND PROTECTION

Cyberstalking is a criminal offense in many countries. In India, Section 66A of the Information Technology Act (before it was struck down) and Section 354D of the Indian Penal Code address online stalking and harassment. However, legal frameworks are often slow to adapt to the rapid growth of digital technologies, and many victims face difficulties in proving their case due to the anonymous nature of the internet.

Countries like the United States have more established laws surrounding cyberstalking, such as the Violence Against Women Act (VAWA), which addresses stalking, both in person and online. However, international cooperation is needed to tackle cross-border cyberstalking effectively.

9. PREVENTION AND SUPPORT

Preventive Measures

To tackle the growing problem of cyberthreats, cyberbullying, and cyberstalking, a multi-pronged approach is required. Individuals can protect themselves by practicing safe online behaviors, such as using strong passwords, being cautious about sharing personal information, and blocking or reporting harmful accounts. Technology companies also have a role in enhancing the security of their platforms, using algorithms to detect and prevent abusive behavior, and providing resources for victims to report harassment. Governments must create and enforce stronger legal protections for online safety, ensuring that laws keep pace with technological advancements. Educational initiatives are vital to raising awareness about the risks of digital harassment and teaching users how to protect themselves.

Mental Health Support and Resources

Victims of cyberthreats, cyberbullying, and cyberstalking need access to psychological support, legal resources, and reporting mechanisms to ensure they are not left to navigate these challenges alone. Public awareness campaigns can also help reduce the stigma associated with being a victim of cyberbullying or cyberstalking. Providing accessible mental health services, counseling, and peer support networks can significantly help victims recover from the emotional and psychological harm caused by online harassment.

10. CONCLUSION

The rise of cyberthreats, cyberbullying, and cyberstalking underscores the urgent need for comprehensive measures to address digital harassment. While the internet offers immense opportunities for connection, it also harbors significant risks that can damage individuals' lives. The cases of Bulli Bai and Sulli Deals are stark reminders of how digital platforms can be exploited to perpetuate gender-based violence, online misogyny, and harassment. Addressing these challenges requires stronger legal frameworks, social awareness, preventive measures, and support systems for victims. Only through collective action can we create a safer online environment for all.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Bulli Bai Case: Mumbai Police Arrest MBA Graduate from Odisha." *The Times of India*, 21 Jan. 2022, www.timesofindia.indiatimes.com.

Abu, Md Sahrom, et al. "Cyber Threat Intelligence – Issue and Challenges." *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 1, Apr. 2018, pp. 371-379,

Amelia, et al. "Changes in Communication Patterns in the Digital Age." *ARRUS Journal of Social Sciences and Humanities*, vol. 3, no. 4, 2023, p. 544, https://doi.org/10.35877/soshum1992

Bada, Maria, and Jason R. C. Nurse. "The Social and Psychological Impact of Cyberattacks." *Emerging Cyber Threats and Cognitive Vulnerabilities*, edited by Vladlena Benson and John McAlaney, Academic Press, 2020, pp. 73-92.

Benson, Vladlena, and John McAlaney, editors. *Emerging Cyber Threats and Cognitive Vulnerabilities*. Academic Press, 20 Sept. 2019.

Hoff, Dianne L., and Sidney N. Mitchell. "Cyberbullying: Causes, Effects, and Remedies." *Journal of Educational Administration*, vol. 47, no. 5, 2009, pp. 652-665.

Ogilvie, Emma. *Cyberstalking. Trends & Issues in Crime and Criminal Justice*, no. 166, Australian Institute of Criminology, 2000, https://www.aic.gov.au/publications/tandi/tandi166.

Pandey, Geeta. "Sulli Deals: The Indian Muslim Women 'Up for Sale' on an App." *BBC News*, 10 July 2021, www.bbc.com/news.

R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu and P. Laplante, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," *IEEE Technology and Society Magazine*, vol. 30, no. 1, pp. 28-38, Spring 2011, doi: 10.1109/MTS.2011.940293.

Slonje, Robert, Peter K. Smith, and Ann Frisén. "The Nature of Cyberbullying, and Strategies for Prevention." *Computers in Human Behavior*, vol. 29, no. 1, Jan. 2013, pp. 26-32.

Wilson, Chanelle, Lorraine Sheridan, and David Garratt-Reed. "What Is Cyberstalking? A Review of Measurements." *Journal of Interpersonal Violence*, vol. 37, no. 11-12, 6 Jan. 2021, https://doi.org/10.1177/0886260520985489