Pakistan Journal of Social Research
ISSN 2710-3129 (P) 2710-3137 (O)
Vol.3, No. 3, September 2021, pp. 130-136
www.pjsr.com.pk

UNDERSTANDING CYBERCRIME AND YOUTH: A PERCEPTION BASED APPROACH

Faiz Ullah
Lecturer, Department of Sociology,
FATA University Darra Adam Khel Kohat, Pakistan
faiz@fu.edu.pk

Ahmad Ali
Assistant Professor, Department of Sociology,
Abdul Wali Khan University Mardan, Pakistan
ahmadalia@awkum.edu.pk

Zahid Umar
Department of Sociology,
Abdul Wali Khan University Mardan, Pakistan
afridiz165@gmail.com

ABSTRACT
In recent years, the issue of cybercrime has overwhelmed everyone who is related to the internet in any capacity. Recent studies have shown that the incidents of cybercrime vastly involve youngsters, which has serious consequences for them as victims and as cyber offenders. The existing body of knowledge related to cybercrime focus upon various issues of internet in general and social media in particular. However, a thorough approach on the issues of cybercrime with relevance to youth is missing. Therefore, this study tries to fill this gap by offering youth and victim-based approach on the issues pertaining to cybercrime. For attaining this purpose, qualitative research approach was adopted in conducting this research project. Semi structured interviews were conducted with 40 young victims of cybercrime. The respondents were recruited through purposive sampling from district Peshawar of 18 to 25 years of age. Furthermore, the respondents were recruited from three clusters of district Peshawar namely Gul Bahar, Hayat Abad, and University town. Various dimensions of cybercrime and involvement of youth as victims and as criminals were explored. It can be concluded that the youth mostly experience cybercrime in the form of cyber bullying, blackmailing and hacking. Further, the findings suggest that many youngsters make their choices on social media and internet without being aware of cybercrimes and thus succumbed to cyber criminals. The participants also reiterated that lack of proper restrictions and policing have created a crime friendly zone for cyber criminals. Based on the findings and participant views, it is recommended that the government, relevant bodies, institutions, and all stake holders including youth should come forward and help in developing a research and technology driven policy backed by separate cybercrime policing system.
Key Words: Cyber space, Cybercrime, Victimization, Cybercriminal, Youth

INTRODUCTION
The last two decades have seen a surge in the use as well as users of internet and digital accessories. The advancement of digital technology has brought numerous benefits like e-services, faster communication and virtual social networking (Arpad, 2013). However, the advancement has also resulted in some serious repercussions such as hacking, scamming, spoofing, cyber stalking, e-theft and cyber criminality (Aiken et al., 2016; Yar, 2006). Collectively, all these repercussions are known as cybercrime. The good image of technology and internet have been threatened by the electronic thefts, frauds and bullying. However, the dominant perspective still represents the internet as the only way of progress, prosperity and socio-economic improvements across the globe (Kamruzzaman, 2016).

Cybercrime has a long history in Pakistan; however, it has been escalated since the inception of third generation (3G) and fourth Generation (4G). These are the faster networks of connecting your phone or device to the internet. These networks facilitate the cybercriminal to siege the cyber space. Cyber space is a virtual arena wherein all cyber activities take place, while cyber criminals are the perpetrators who utilize technology and cyber space as means to commit cybercrime. Cybercrime includes hacking, cyber theft, blackmailing, and cyber terrorism (Ullah, 2018; Yar, 2004). Even though, the issue of cybercrime is not new, but its' escalation in the past decade has compelled the government of Pakistan to make effective laws (Khan, 2016). Consequently, the government, while reforming the existing cyber laws, has introduced a new bill called Pakistan Electronic Crime Act (PECA) in 2016. This bill aimed to criminalizes the various forms of cyber misdeeds including cyber terrorism and child pornography. In response to PECA, the human rights commission of Pakistan (HRCP) has termed it infringement on the freedom of expression. The HRCP voiced their concerns that the government and law enforcement agencies might misuse it for their gains (Hassan, 2016). Yamin (2021) argues that the issue of cybercrime has still been at the bottom of interest for Pakistan therefore, we are behind other nations when it comes to curbing and preventing cyber-attacks.

Amongst the current 61.34 million users of internet in Pakistan, about 46 million are social media users (Datareportal, 2021), which includes a major portion of youngsters who use social media for attaining information, learning, fun, social networking or time killing. The social media works bidirectional for youth as victims and offenders of cybercrime. For example, many incidents of cybercrime in Pakistan involve youngsters who hack, stalk, or steal online. On the other hand, many youngsters fall prey to cyber criminals due to lack of proper information regarding various social media sites, web, and applications. Recently, a young lady was apprehended by the Federal Investigation Agency (FIA) for hacking a private newspaper website (TN, 2017). Another case pertaining to cybercrime occurred in a renowned college in Khyber Pakhtunkhwa (KP) wherein a student defamed his female teacher by hacking her social media account and later sharing obscene material form that account (Ahmad, 2016).

Cybercrime is the result of expanded internet web and its' transformation (Castells, 2002). Generally, the issue of cybercrime receives less attention due to the absence of any injuries and physical losses. However, recently, the rate of cybercrime has been escalated as FIA registered mora than 15000 cases in 2019 and 100000 in 2020. Still, cybercrime receives less attention because hacking, stalking, and cyber threats are considered as less important and far from reality (Yar, 2006). The youngsters barely try to get the relevant information about the social media sites, websites, or applications they are using or giving access to (Arpad, 2013). The alleged safety and protocols assure the users that they are secure form any kind of cyber misdeed however, any cyber hassle can happen even within seconds.

LITERATURE REVIEW

Recent years have seen a drastic increase in the crimes which involves information technology however, in comparison, the rate of physical crimes decreased (Kranenbarg et al., 2017). Due to the unique nature and space of cybercrime, it has overwhelmingly attracted the attention of Sociologists and Criminologists (Webster, 2003; Holt et al., 2019). The internet has influenced almost every section of the society including social, religious, cultural, and personal spaces. However, this influence has induced a huge problem in the form of cybercrime, especially for a developing country like Pakistan. It has posed a major threat to individuals, businesses, organizations, and other users across cyber space. Unlike other forms of crime, this threat has exacerbated the entire structure of stable patterns in the society. Youngsters involved in cyber activities are considered as deviants by various sections of the society. On the other hand, majority of the youth do not pay any heed to attain basic and required knowledge before using or logging into a cyber space or platform like social media sites and websites. This negligence has pushed many youngsters into the cyber-chaos.

The exponential expansion of internet has changed the very dynamics of societies worldwide, affecting almost anybody who has access to it. It has transformed many spheres of life and the transformation is continuously growing (Castells, 2002). The process of globalization has involved other factors too but, the main actor is the internet which is bringing about new changes and challenges. These changes are going to pose a threat to the society as well as bring some beneficial aspects that represents a

new digital era (Webster, 2003). This digital era is sliding to prove what Beck (1998) called "Risk Society". All these changes and transformations brought by technological advancements have been resulted in criminal and deviant offences. On one hand, the digital advancement has been regarded as inevitable and lifesaving, but on the other hand it has painstaking repercussions for youth (Critcher, 2003)

The criminal activities attached with the cyber space are sometimes overrepresented by the mass media. Consequently, this overrepresentation makes some people to avoid cyber activities, and some youngsters to adapt cyber activities for committing new crimes (Goode & Ben-Yahuda, 2010). Thomas and Loader (2010) believed that the transformation of social fabric by the internet and its' latest altercations have made people to think of internet as a genuine threat to the smooth functioning of society. The contemporary attachment of youth with the online gaming and social media activities have made them more susceptible to online crimes. Vegh (2002) argues that the hype created by series of cyber crimes highlights the balanced understanding and importance of cyber misdeeds. However, a balanced and understandable view of cybercrime is extremely necessary for turning fantasies into realities (Critcher, 2003).

The general ratio of cyber victimization may be low however, it is highly concerning among the young users (Nasi et al., 2015). According to Muhammad et al., (2021), cybercrime is a harmful activity for victims which badly affects the persons who bear weak ties in society. It is also noted that the youngsters who indulge in cyber activities for most of their time are very much distracted from their mainstream society as well as their peers. The study conducted by Goldsmith and Wall (2019) explores the role of internet and cyber space in turning the youth into offenders. They argue that due to its' ease and accessibility, cybercrime space has made the youth more adrift towards the cyber criminality (see also Goldsmith & Brewer, 2015; Alter, 2017).

The rate of cybercrime victimization is high amongst the young groups compared to the old age groups. It has been argued that this rate is going upward each year (Nasi et al., 2015). The fact of the matter is that youngsters excessively use technology and stay online for most of their time that increases the chance of their victimization (See Ybarra, 2004). However, there are numerous factors that propel the youngsters to be victimized i.e, lack of technological knowledge and the use of unprotected or under-secured sites. Some sites and applications have weak security protections and protocols, which are vulnerable to cyber-attacks and malwares. It is argued that in most of the cybercrime cases, youth put themselves at risk because of their own shortcomings (Livingstone et al., 2013). On the other hand, Oslo (2017) argues that the youth, who commit cybercrimes, are facing poverty, frauds, joblessness, greediness in their life and they consider cybercrime as an easy way of attaining wealth without taking any physical risks.

Pakistan also faces the risks and threats of cybercrime and Federal Investigation Agency (FIA) and Police are arresting cyber criminals from Bahawalpur and Peshawar including gangs and young university going students (Manzar et al., 2016). The internet users in Pakistan do not pay heed to cyber threats, only some of the victims profess its' urgency and prevention. The habits of cyber criminals and misuse of technology can be coped with the ban on various websites, channels and sources to deal with cyber criminals in Pakistan (Ahmed & Khan, 2015; Munir & Gondal, 2017). The incidents of cybercrime in Pakistan ranges from sending offensive text messages to cyber pornography (Munir & Gondal, 2017).

RESEARCH QUESTION

What is the perception of youth about cybercrime in Pakistan?

OBJECTIVES OF THE STUDY

- To explore the phenomenon of cybercrime amongst youth in Pakistan.
- To investigate the perception of youth about cybercrime.

MATERIALS AND METHODS

This study has been conducted through a qualitative approach. Interpretive paradigm has been employed to probe the various dimensions of youth and cybercrime. For this project, a total of 40 semi structured in-depth interviews were conducted with young victims of cybercrime. The participants were recruited through purposive sampling. The criteria of inclusion for participants was that one must have experienced

cybercrime in any form, for instance, blackmailing, cyber bullying, defamation or hacking. Furthermore, young victims of cybercrime were targeted and recruited to justify the purpose and rationale of the study. The participants were recruited from district Peshawar; however, the rationale for recruiting participants was that district Peshawar has vast internet accessibility compared to other districts of Khyber Pakhtunkhwa. Various concepts related to cybercrime, youth, impacts of cybercrime on youth, victimization, and youth's perception were addressed in the interviews while some concepts were beyond the scope of this article. The interviews were conducted in Pashto and were later translated and transcribed in English. The 40 interviewees were victims of different types of cybercrime including hacking, stalking, and e-frauds. The collected data have also been supported by documents, reports, and newspaper articles. The participants age was from 18 years to 25 years. The interviews were transcribed and then analyzed through Hammersley (2015) approach.

RESULTS AND DISCUSSION

For a developing country like Pakistan, cybercrime is becoming a nuisance with every passing day. The use of internet and technology is growing, which is giving rise to cyber space users as well as cyber criminals. The youngsters use different internet-based platforms even without attaining proper knowledge or understanding before its' use. On the other hand, the cyber space has provided a criminal friendly environment because of its' anonymity as the user or criminal can his identity or disguised it. Anyone can commit a crime without revealing their real details on the internet-based platforms i.e., Facebook, email, twitter, websites, or other channels. No internet platform requires verified identity because of their procedural requirements. This loophole has given rise to incidents of cybercrime and is therefore griming the good use of cyber space in the society. Majority of the respondents stated that cybercrime mostly involve the de-identified crimes by people who easily keep their identity undisclosed and ironically, they easily got away with their crime. In conventional crimes, you have a victim and a criminal which can easily be identified from the evidence at the place of crime, but in case of the cybercrime, you do not have any clue whether you have been targeted from within or outside the country.

A respondent quoted that,

"Cybercrime comprises of any act that are directed to target a person's computer system, phone or their electronic gadgets knowingly on purposely or without any reason. It involves targeting small businesses to banks, reputed organizations, and affluent people. Larger organizations, businesses, and affluent people can pursue their cases and criminals but general public face a lot of difficulties while reporting a case to concerned institutions"

One victim of the cybercrime told the researcher that,

"Cyber offences are the actions usually committed by the people whom you do not know. For example, when my account was hacked, I did not know that why my account has been hacked."

One respondent stated that,

"*I was chatting to this person who was using female identity, I shared my secret pictures and videos and then he started blackmailing me for money. He threatened me if I don't send money, he will share all the material on Facebook".*

Another respondent told the researcher that,

"My account was hacked, and the hacker shared obscene pictures with almost all my friends including my relatives, which was a moment of great embarrassment for me as they did not know initially that my account has been hacked".

Before experiencing cybercrime, many of the youngsters perceive it as non-existent and self-proclaimed; however, the victims realized the seriousness and the threats that cybercrime can pose as soon as when they encountered it by themselves. Majority of the victims experienced cybercrime in the form of cyber bullying, stalking and hacking. However, some of the respondents were also defamed in malicious campaigns against them by sharing various propaganda materials om different social media platforms, while some of the respondents has experienced financial crimes of hacking money.

The respondents also opined that the general society and even the law enforcement agencies consider the cybercrime less important and therefore they do not investigate many cases to their logical

conclusions. Consequently, the cyber criminals are getting encouraged and they are coming up with barrage of cybercrime on individual, organizational, and professional basis. The criminals are diligently using the lack of knowledge vulnerability amongst our youth, one user told the researcher that I started using Facebook on a friend's suggestion without even knowing a single fact about the facebook or its' use. On the hand, criminals make fake profiles, use fake proxies and multiple different IPS to target various users.

To conclude the debate, it is argued that internet and its' allied facilities and applications have overwhelmingly impact on all the dimensions of social life. Cybercrime is a dilemma for the society and the youngsters themselves. Islam (2015) believed that youth with latest knowledge of different cyber platforms make use of the cyberspace in a fruitful and meaningful way; however, people with inadequate knowledge will mostly keep using it for the fun and unnecessary activities hence, giving rise to the cyber misdeeds. To sum this up, most respondents argued that the cyber space is not bad rather its' use by the youth makes it either good or bad. Some respondents said that the use of internet should be avoided by the youth, they were skeptical of the internet use because of the incidents that happened to them, and they further responded that proper trainings or guidance should be sought and given to the youth before their exposure to the vulnerable world of internet and cyber space.

One of the respondents told the researcher that,

"People think of cyber criminals as unknown people but in most of the instances, they would knowingly target you for something. If you do not know those people through internet you may later came to know that they know you in real life".

Another respondent stated that,

"I think mostly criminals commit cybercrime because you are an easy target for them and the reasons can BE numerous like your lack of knowledge, interest or even your device that you are using."

According to the youth, who had experienced the cyber misdeeds, our society consider cybercrime as anonymous and do not give the required importance and attention and resultantly, cyber criminals are taking advantage of this. For wide recognition and obliteration of the cybercrime, thorough programs of awareness and trainings is the need of the hour. Otherwise, it will ostensibly become hard to curb and flatten the exponentially rising rates of cyber incidents. It is indeed needed that every concerned person should take the issue of cybercrime serious and play their part on every forum where required. According to the major portion of the victimized respondents, the government and civil society should come forward to create awareness against countering this menace. Rigorous programs should be launched to alter the perception of the masses about the social media, internet**,** and its' allied facilities to help in reducing the cyber victimization of our masses in general and youth in particular.

One respondent argued that,

"It is your activities that makes you vulnerable if you are abundantly using the internet and social media sites, it is more likely that you will fall in the trap of cybercrime. The criminals come with a mindset and target people because they are not observed or checked by anyone due to the anonymity offered by the cyber space."

Many researchers studying online crime have utilized the Cohen an Felson (1979) Routine Activity Theory (RAT) (Reyns et al., 2011; Wick et al., 2017; Aizenkot, 2021), which argues that situation of crimes involve a motivated offender and a target. Hence, young cybercriminals are motivated by specific aims like money, insult, revenge, or something else. Furthermore, a crime for instance, cybercrime will most likely occur when there is an accessible target, absence of guardian and a motivated criminal. Based on RAT, it can be concluded that in case of cybercrime amongst youth, cyberspace provides an easy, accessible and vulnerable targets while the criminals are motivated due to personal, professional or financial reasons; a student targeting teacher, a colleague targeting other colleagues and sometimes a user of one platform targeting another user of the same platform.

CONCLUSION

An extensive body of knowledge focus on the involvement of youngsters in cyber activities across the youth dominated cyber space. In this study, we focused on the issues related to cybercrime amongst youth. We argue that cybercrime is a two-way process for youth as they are victims as well as criminals of cybercrime.

It is concluded that the main reasons for victimization of youth are lack of knowledge, lack of interest in understanding the sites, and taking the cyber space as a protected zone. Cybercrime can be found vastly in the form of cyber bullying, stalking and hacking. In some instances, it can also be found in the form of defamation, cyber pornography and cyber terrorism. The victims of cybercrime are treated as 'not victims' rather they are blamed for their victimization because cybercrime is considered as victim's fault. On the other hand, cybercriminals enjoy a lot of freedom due to insufficient and ineffective cyber laws in our country, the criminals can easily go away with serious cybercrimes. In many cases, cyber criminals cannot be tracked because of their unique use of technological sources including the IP address. To curtail the freedom and power of cyber criminals, the government and all stake holders need to come up with a latest cyber knowledge driven policies backed by the technologically equipped and separated cyber police which should only deal with cyber affairs in the country.

LIMITATIONS AND FUTURE DIRECTIONS

The data has been collected from the youth only; hence, its' results cannot be generalized on people other than youngsters. The other obvious limitation is universe of the study, which has been confined to only three clusters of district Peshawar. The questions asked were only limited to how the youth perceive cybercrime and cyber criminals.

As the results of the study indicates that youngsters are victims as well as offenders of the cybercrime. For future studies, the mental health and well-being of the youth can be considered as peoples' mental health and well-being play an important in the society. Moreover, other themes like socio-economic impacts can also be probed in regard to cybercrime in Pakistan.

REFERENCES

Alter, A. (2017). *Irresistible: Why We Can't Stop Checking, Scrolling, Clicking and Watching*. Bodley Head.

Ahmed, A., & Khan, D.S. (2015). Cyber Security Issues and Ethical Hacking in Pakistan. Department of Computer Science Karachi University.

Ahmad, N. (2016). *A Student of ICP Arrested by FIA.* Pro Pakistani.

Aiken, M., Davidson, J., & Amann, P. (2016). Youth pathways into cybercrime.

Árpád, I. (2013). A greater involvement of education in fight against cybercrime. *Procedia-Social and Behavioral Sciences*, *83*, 371-377.

Aizenkot, D. (2021). The predictability of routine activity theory for cyberbullying victimization among children and youth: risk and protective factors. *Journal of interpersonal violence*.

Beck, U. (1998). 'Politics of Risk Society. In. Pepper, D., Webster, F., Revill, G. *Environmentalism: Critical Concepts*, 256-266.

Castells, M. (2002) *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford University Press.

Critcher, C. (2003) *Moral Panics and the Media*. Open University Press.

Goldsmith, A, Brewer, R (2015) Digital drift and the criminal interaction order. theoretical criminology *19*(1), 112–130.

Goldsmith, A., & Wall, D.S. (2019). The seductions of cybercrime: adolescence and the thrills of digital transgression. *European Journal of Criminology*.

Goode, E., & Ben-Yehuda, N. (2010). *Moral panics: The social construction of deviance*. John Wiley & Sons.

Hamersley, M. (2015). Sampling and thematic analysis: A response to Fugard and Potts. *International Journal of Social Research Methodology*.

Holt, T. J., Brewer, R., & Goldsmith, A. (2019). Digital drift and the "sense of injustice": Counter-productive policing of youth cybercrime. *Deviant Behavior*, *40*(9), 1144-1156

Kamruzzaman, M., Islam, M. A., Islam, M. S., Hossain, M. S., & Hakim, M. A. (2016). Plight of youth perception on cybercrime in South Asia. *American Journal of Information Science and Computer Engineering*, *2*(4), 22-28.

Kranenbarg, M., van der Laan, A., De Poot, C.J., Verhoeven, M., van der Wagen, W., & Weijters, G. (2017). Individual cybercrime offenders. *Research agenda: The human factor in cybercrime and cybersecurity*, 23-32.

Khan, R. (2016). *Cyber crime bill passed by NA: 13 reasons Pakistanis should be worried*. *Dawn*. Livingstone, S., Ólafsson, K., & Staksrud, E. (2013). Risky social networking practices among "underage" users: lessons for evidence-based policy. *Journal of Computer-Mediated Communication*, *18*(3), 303-320. Manzar, U., Tanveer, S., & Jamal, S. (2016). The incidence of cybercrime in Pakistan.

Munir, A., & Gondal, M.T. (2017). Cyber Media and Vulnerability: A discourse on cyber laws and a probe on victimization of cybercrimes in Pakistan. *Global Media Journal: Pakistan Edition*, *10*(2).

Muhamad, F. H., & Muhammad, M. Z. (2021). Awareness on Financial Cybercrimes among Youth: Experience, Exposure and Effect. In *First International Conference on Society 5*.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *16*(2), 203-210.

Ojolo, T. (2017). *Youth perception on yahoo-yahoo (cybercrime): a case study of Ado-Ekiti, Ekiti State Nigeria* (Doctoral dissertation).

Reyns, B.W., Henson, B., Fisher, B.S. (2011). Being pursued online: Applying cyberlife style-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169.

Shah, S. (June 21, 2016). An Analysis of Pakistan's new cyber-security law. *The News.*

N.a, (October 08, 2017). Man in Chitral Arrested For Hacking. *The News.*

Thomas, D. and Loader, B. (2000). 'Introduction – Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. Routledge.

Ullah, F. (2018). Socio-psychological impacts of cybercrime on youth: A case study of Peshawar, Khyber Pakhtunkhwa [Unpublished Master of Philosophy dissertation] University of Peshawar.

Vegh, S. (2002). 'Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking'. *Retrieved from:* online at http://firstmonday.org/issues/ issue7_10/vegh/index.html

Webster, F. (2003). *Theories of the Information Society*. Routledge.

Wick, S. E., Nagoshi, C. T., 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), 24–39.

Yar, M. (2006). *Cybercrime and society: Analysis of motivation and typology*. Sage Publications.

Yamin, D. (2021). Cyberspace Management in Pakistan. *Governance and Management Review*, *3*(1).

Ybarra, M.L. (2004). Linkages between depressive symptomatology and Internet harassment among young regular Internet users. *Cyberpsychology & Behavior,7*, 247–257.