Vol-X, Issue-II, Fall 2017
ISSN: 2070-2469
HEC RECOGNIZED
http://www.aiou.edu.pk/SAB/gmj/
Global Media Journal
Pakistan Edition

Cyber Media and Vulnerability: A discourse on cyber laws and a probe on victimization of cybercrimes in Pakistan

Asad Munir

Maryam Tahira Gondal

Abstract

Internet has given birth to new media technologies and social media. This study is planned to explore whether there is any relation between the usage of social media and vulnerability to be a victim of cybercrimes. The study will also investigate the current trends of cybercrimes, the extent of awareness about cybercrimes, attitudes about cybercrime reporting, perceptions about cybercrime laws and impact of cyber laws in Pakistan.

Social media is now a personal medium for expression of personality and is extensively used tool for interpersonal communication, group as well as mass communication. People across the globe take keen interest in social networking for their routine communication as well as for information and entertainment. On the other hand certain people, groups or organizations are cleverly using this medium for their black and grey propaganda, cybercrimes and malpractices involving criminal procedures and targeted actions against individuals and organizations. Easy access to social media has empowered the criminal minds to use this medium to adopt new ways of fraudulent activities, thefts, harassments and terror. It is need of the time to measure if the social media users are aware of common cyber crimes and whether they are versed with the

precautionary measures and if the report the crimes to law enforcing agencies or not. The study was aimed to investigate the level of awareness on cyber crimes in Pakistan as well as the public perception on cyber laws. The study further investigates the relationship between the amount of time spent on cyber media and vulnerability to fall a victim to the cybercrimes.

Keywords: *Cyber Media, Social Media, Cybercrimes, Cybercrimes in Pakistan, Cyber Laws*

Introduction

What is cyber communication?

Cyber media or digital communications is the term applied to communication that is facilitated by the Internet but also through multimedia advances such as, flash storage, high definition broadcasting, CD ROMs etc. (Servine & Tankard, 2001)

According to Wiktionary, the term cyber media refers to the publishing through internet or cyberspace.

Characteristics of Cyber Media

Dizard (1997)described that cyber media may expand the range of resources to so many new dimensions; such as, they can provide online interactions and links between the consumer and the information-provider.

Manovich (1999)presented four major characteristics of cyber media i.e.

i) Numerical Representation

ii) Modularity

iii) Automation

iv) Variability

Vol-X, Issue-II, Fall 2017
ISSN: 2070-2469
HEC RECOGNIZED
http://www.aiou.edu.pk/SAB/gmj/
Global Media Journal
Pakistan Edition

What is cyber crime?

Oxford Advance Learner explains cyber crime as crime committed by the use of Internet, such as by stealing someone's personal or bank details or causing problems in their computer with viruses etc. Cybercrimes may be committed through the use of computer and internet.

Cybercrime is criminal action done utilizing PCs and the Internet. This incorporates anything from downloading unlawful music, documents, stealing dollars from online financial balances etc. Cybercrime likewise incorporates non-fiscal offenses, for example, making and dispersing infections on different PCs or posting secret business data on the Internet.

Types OF CYBERCRIME:

1. Against Individuals

i.Drugs trafficking

ii.Hostile Content and Harassment

2. Against Individual Property

i. Electronic Funds Transfer Fraud

ii. Dispersion of Offensive Materials

3. Against Society

i. Digital tormenting and Cyber-stalking

4. Against Private Organizations

i. Stealing telecommunication services

ii. Piracy against telecom organizations

5. Against Government/country

i. Electronic Vandalism and Extortion

ii. Digital Warfare and Terrorism

Vol-X, Issue-II, Fall 2017
ISSN: 2070-2469
HEC RECOGNIZED
http://www.aiou.edu.pk/SAB/gmj/
Global Media Journal
Pakistan Edition

Cyber laws in Pakistan

Cyber laws or, less colloquially, web regulation, is a time period that encapsulates the authorized issues regarding use of communicative, transactional, and distributive elements of networked devices and technologies. With the passage of time, different laws were promulgated such as:

- The Telegraph Act, 1885,
- The Wireless Telegraph Act, 1933,
- The Electronic Transaction (Re-organization) Act, 1996,
- Electronic Transaction Ordinance 2002,
- The Payment Systems and Electronic Fund Transfers Act, 2007,
- Prevention of Electronic Crimes Ordinance, Pakistan 2007,
- Prevention of Electronic Crimes Ordinance, Pakistan 2008

These are the legal guidelines beneath which communication; transactions, expertise, files, and files in digital type are ruled over internet and to give accreditation to the electronic transactions, understanding, records, communiqué and transactions as legitimate piece of evidence to the correspondence. The offences under these laws are non-bail able, non-compoundable and shall no longer are trying in any inferior court rather thanthe sessions court. In case if the act achieved is under the digital Fund Transfers Act, 2007 then there is a civil suit with by the competent court through determining the pecuniary jurisdiction with reference to the controversy.

Electronic Transaction Ordinance, 2002

Cyber laws were made in the reign of Pervaiz Musharraf named as Electronic Transaction Ordinance 2002.This was the first legislation by national lawmakers of Pakistan. There are 43 sections in this ordinance.Important Sections are:

Section 36. Violation of private information

Information or attempting to gain access to any information system with or without intent to acquire the information may lead to a penalty of imprisonment for 7 years or with a fine of Rs. 1 million or both.

Section 37. Damage to the information system

Altering, modifying, deleting, removing, generating, transmitting or storing information to impair the operation of, or prevent or hinder access toinformation knowingly is not authorized. It may lead to imprisonment for 7 years or with a fine of Rs. 1 million.

Section 38. Offences non bail-able, compoundable and cognizable

All the offences under this Ordinance shall be non bail-able, compoundable and will be cognizable.

Cyber crimes defined under the law arean activity in which computer or digital gadgets are used or targeted or place of criminal activity.There are many types of cyber crime such as:

- Stealing the Identities
- Committing Frauds
- Violating Privacy

In 2007, the government increased the jurisdiction of cyber law and introduced Electronic Crime Bill.It was promulgated by the President of Pakistan with effect from 31st December 2007.

Prevention of electronic Crimes Ordinance, 2008

This law is in force now, which was promulgated by the President of Pakistan. The Prevention of electronic Crimes Ordinance 2008 extends to the whole of Pakistan.

The Prevention of electronic Crimes Ordinance, 2008 applies to every person who commits an offence under the stated Ordinance without reference to his nationality or

citizenship whatever or in any position outside or within Pakistan, having dangerous outcomes on the safety if Pakistan or its nationals or country wide concord or any property or any electronic system or knowledge located in Pakistan or any electronic process or information ready of being linked, sent to, used by or with any electronic approach in Pakistan.

The ordinance gives exceptional powers to the Federal Investigation Agency (FIA) to investigate and charge circumstances in opposition to such crimes.

The ordinance covers provision for unlawful and crook acts like data access, system damage, data damage, electronic forgery, electronic fraud, spoofing, spamming, cyber terrorism etc.

Chapter II of the Prevention of electronic Crimes Ordinance, 2008 offers with the Offences and Punishments. Punishments vary from two years to demise penalty. For the overall steering offences and punishments are stated below:

section 3 of the Prevention of electronic Crimes Ordinance, 2008 deals with criminal access: The stated section states crook access as:

Whoever deliberately gets unauthorized access to the entire or any part of a digital process or electronic gadget with or without infringing protection measures, will be punished with imprisonment of both for a term which can prolong to 2 years or with no longer exceeding 300 thousand rupees, or with each. Criminal access to data is Offence and Punishable.

Section four of the Prevention of Electronic Crimes Ordinance, 2008 states illegal data access:

Whoever intentionally motives any digital procedure or electronic device to participate in any function for the intent of gaining unauthorized entry to any information held in any digital system or digital gadget or on acquiring such unauthorized entry will probably be

punished with imprisonment of either for a term which may prolong to three years or with fine or both.

Prevention of Electronic Crimes Ordinance, 2008: section 5 definesDamage to Data:

Whoever with intent to unlawful access or intent harm to the public or anyone, damages any information will probably be punished with imprisonment of either for a term which may prolong to 3 years or with fine or with each.

Prevention of electronic Crimes Ordinance, 2008: section 6 states Damage to System:

Whoever with intent to damage to the general public or anyone interferes with or interrupts or obstructs the functioning, reliability or usefulness of a digital system or electronic device with the aid of imputing, transmitting, detrimental, deleting, altering, tempering, deteriorating or suppressing or offerings or halting digital process or choking the networks shall be punished with imprisonment for a term which may lengthen to three years or with huge fine or with each.

Prevention of Electronic Crimes Ordinance, 2008: part 7 states electronic fraud:

Whoever for wrongful gain interferes with or makes use of any information, electronic procedure or electronic gadget or induces any individual to enter right into a connection or with intent to deceive anybody, which act or omissions is likely to damage to that person or every other person will likely be punished with imprisonment for a term which may extend to seven years, or with fine, or both.

Prevention of Electronic Crimes Ordinance, 2008: part eight addresses Electronic Forgery:

Whoever for wrongful purpose interferes with data, digital method or electronic gadget, with intent to cause injury or harm to the general public or to anybody, or to make any unlawful claim or title or to purpose someone to phase with property or to enter into any specific or implied contract, or with intent to commit fraud by means of any input,

alteration, deletion, or suppression of information, resulting in unauthentic information with the intent that it be regarded or acted upon for authorized purposes as if it were professional, in spite of the truth that the info is instantly readable and intelligible or no longer will likely be punished with imprisonment for a term which may lengthen to seven years, or with fine or both.

Prevention of Electronic Crimes Ordinance, 2008: Section 9 describes Misuse of digital system or electronicequipment

Everyone who produces, possesses, procures, sells, transports, imports, distributes or makes on hand an electronic system or digital device, together with a software, designed or adapted notably for the purpose of committing any of the offences established beneath this Ordinance or a password, entry code, or an identical data by which the entire or any part of an digital procedure or digital device is capable of being accessed or its functionality compromised or reverse engineered, with the intent or not it's used for the purpose of committing any of the offences that are under this ordinance, is alleged to commit of misuse of digital process or digital gadgets. Whoever commits the offence shall be punishable with imprisonment of either description for a term which may lengthen to three years, or with fine, or both.

Prevention of digital Crimes Ordinance, 2008: section 10 states Un-authorized access to code:

Whoever discloses or obtains any password, entry as to code, system design or some other means of gaining entry to any electronic system or data with intention to acquire wrongful goals, do reverse engineering o for loss to some other or any other illegal intent will be punished with imprisonment of either for a time period which may extend to three years.

Prevention of Electronic Crimes Ordinance, 2008: section eleven defines Misuse of encryption:

Whoever for the motive of an offence or concealment of incriminating evidence, with knowledge and willfully encrypts any communication or data or knowledge contained in electronic system commits the offence of misuse of encryption shall be punished with imprisonment of both description for a term which can extend to 5 years or with fine or with both.

Prevention of electronic Crimes Ordinance, 2008: Section 12 states malicious code:

Whoever willfully writes, offers, makes available, distributes or transmits malicious code by means of a digital system or electronic device, with intent to harm any electronic process or ensue in the corporation, distribution, suppression, alteration, theft or lack of data commits the offence of malicious code. Provided that the supply of this part shall no longer practice to the authorized testing, research and progress or safeguard of an electronic process for any lawful intent.Whoever commits the offence will probably be punished with imprisonment of either for a term which may extend to five years, or with fine or with both.

Prevention of electronic Crimes Ordinance, 2008: Section 13 states Cyber stalking:

Whoever with intent to coerce or harass anyone else who makes use of pc, network, web, community website, electronic messaging or every other similar approach of verbal exchange to be in contact obscene, vulgar, profane, lewd, lascivious, or indecent language, photograph or image, makes any suggestion or idea of an obscene nature, threaten with any unlawful or immoral act, takes or distributes photographs or portraits of anyone without his consent, displays or distribute expertise in a way that appreciably raises the danger of damage or violence to some other person, commits the offence of cyber stalking.

Prevention of electronic Crimes Ordinance, 2008: section 14 states Spamming:

Whoever transmits detrimental, fraudulent, misleading, illegal or unsolicited bulk electronic messages to someone without the categorical permission of the recipient, or causes any electronic system to show this sort of message or makes a falsified online user account registration or falsified domain title registration for commercial purposes commits the offence of spamming.

Prevention of electronic Crimes Ordinance, 2008: section 15 defines Spoofing:

Whoever makes a website, or sends a piece of email with a counterfeit source to be believed by means of the recipient or visitors or its digital system to be a legit source with intent to achieve unauthorized access or obtain valuable expertise which later can be utilized for any lawful functions commits the offence of spoofing.

Prevention of Electronic Crimes Ordinance, 2008: section sixteen states Un-authorized interception:

Whoever without lawful authority intercepts by means of technical method, transmissions of data to, from or inside an digital process together with electromagnetic process carrying such information commits the offence of unauthorized interception.

Prevention of Electronic Crimes Ordinance, 2008: Section 17 states Cyber terrorism:

any individual, workforce or organization who, with terroristic intent utilizes, accesses or means to be accessed a pc or computer network or electronic system or electronic gadget or by way of any to be had approached, and thereby knowingly engages in or makes an attempt to engage in a terroristic act commits the offence of cyber terrorism.

Prevention of electronic Crimes Ordinance, 2008: part 21 states Offences via Corporation:

A company or body will probably be held responsible for an offence under this Ordinance if the offence is dedicated on its instructional materials or for its benefits. The company

will be punished with heavy fine at minimum of 100 thousand rupees or the amount concerned within the offence whichever is the larger provided that such punishment shall no longer absolve the illegal action of the person who has done the offence. Corporation entails a body of persons included beneath any law comparable to a trust waqf, an association, a statutory structure or a company itself.

Government's Proposed and Modified Cybercrime Bill 2015

This bill has already been approved from the committee of national assembly and is yet to be placed for the final approval. There are 5 main points of concern by summarizing the new bill as mentioned by (5 Main Points of CyberCrime Bill, 2015) which are as under:

1. It is going to be a criminal offense to send text messages or snap shots to anybody's e mail or cellphone without the recipient's consent.

2. The police or FIA or some other agency will not need a warrant to look, grab or make arrests of anyone.

3. Under sections 17 and 18 of the new bill suggest that the political criticism and expressing political opinions within the type of analysis, commentary, blogs, cartoons, caricatures and memes has be considered a crime. Authorities will decide what's ethical and what is not.

4. Under section 31, the executive can block or restrain access to any website or online source if it deems it inappropriate.

5. Under section 26, the internet service providers, eating places, shops, hotels, offices, airports bus stations and wherever with internet facility is given, will be required to preserve information for 3 months.

FIA's National Response Centre for Cyber Crimes

National Response Centre for Cyber Crimes was established by Federal Investigation Agency Pakistan to deal with technology based crimes. The Centre commonly known as

NR3C provides the services of Digital Forensics, Technical Investigation, Penetration Testing, Training and Information System Security Audits.

Reporting a cybercrime

Cybercrime can be reported online through the website of NR3C i.e. www.nr3c.gov.pk by providing the complainant's name, parentage, gender, phone number, CNIC number, email, address and crime's details. The victims may also visit the regional NR3C offices.

Jurisdiction of NR3C

NR3C entertains the crimes like:

- Unauthorized accessed electronic data or identity
- Email hacking or Fake User IDs
- Online Scams and Frauds of monetary nature
- Defamation on cyber media

Review of Literature

Cybercrimes increased in incidence and their complexities in the era of 1990-2009. In the beginning on the hacking was considered as a cybercrime which was challenging the intellectual properties. In 1990s the phenomenon developed further and personal computers and other digital gadgets started becoming more sophisticated. New types of criminals also started emerging and they started exploiting and internet users became more vulnerable to crimes. Phone phreaking also evolved enormously (Brenner, 2010).

Even as females benefit from new digital and web technologies for self-expression, networking, and legitimate movements, cyber victimization remains an underexplored barrier to their participation. Women in general, outnumber guys in surveys on cyber victimization."Cyber Crime and the Victimization of ladies: laws, rights and rules"isa specified and foremost contribution to the literature on cyber crime. It explores gendered

dimensions of cyber crimes like grownup bullying, cyber stalking, hacking, defamation, pornography,graphics, and electronic blackmailing. These and different techniques designed to inflict intimidation, manage, and other harms are generally committed through perpetrators who, for a lot of reasons, are unlikely to be recognized or punished. Scholars, researchers, law makers, and average women and their supporters will attain a greater understanding of cyber victimization and detect the best way to reinforce responses to cyber crimes against ladies (Halder & Jaishankar, Cybercrime and the Victimization of Women: Laws, Rights and Regulations, 2011).

While studying the college students of Kolkata who were members of social networking websites, it was revealed that many of them were victims of cyber stalking and harassment and in many cases the stalkers were anonymous and had no personal information in their profiles. The options of anonymity have added to the criminal activities associated with the internet and cyberspace and criminals are free to use social networking websites to stalk and threat the people. Technology Act 2008 of India never addressed the issue(Sen A. , 2013).

In ancient times the teachers were given huge respect and they enjoyed a prime space in student's life. Whereas now the students in age group 12-24 are targeting the teachers through cyber media to bully, threat, defame and spread hatred against their teachers. They are finding internet a way to victimize their teachers on social websites either due to their frustrations or for personal favors and demands from their teachers. The perpetrators vent out their frustration and anger over the teachers in very abusive language and also gather sympathies. Internet service providers often do not provide any assistance to the victims and the victims also don't try to involve police in most of the cases, thus the crime keeps rising (Halder &Jaishankar, 2013).

India has a new law that is based on evidence that considers admissibility, accuracy, authenticity and sufficiency to convince the judiciary about the crime. The actual challenge in cyber crime cases is getting that evidence that can stand scrutiny in a foreign court as well. As per the report of National Crime Records Bureau, total 179 cases of cyber crimes were registered in the year 2005 under the IT Act 2000 of India, and 50$ of the cases were regarding the publication of obscene material or pornography. 125 people were arrested(Kumar A. P., 2009).

Another very likely security risk on e-banking includes the identity theft such as through phishing and spoofing. Phishing involves sending such emails which look from some authentic organizations which trick the consumers to give their password and other personal details by replying to those emails. Spoofing involves use of fake websites which often make customers believe they are surfing the real website. Other risks involve the risks of transactions, credit risks, monetary risks and risks like legal compliance (Mambi, 2010).

Conclusive attribution of cybercrimes or cyber attacks is impossible. Cyber warfare is a legal grey area. Industries can be a major target of cyber attacks. The main actor in state sponsored cyber operations is the cybercrime. To fight against this challenge, it is required to hold public debates, establish confidence building measures, improve general IT security, introduce smart and appropriate regulations, focus on the resilience, keep a look over the risks of backdoors, secure the supply chain systems, prefer open source instead of proprietary alternates and above all; not trading the security over the freedom of speech (Kosina, 2012).

Some important measures towards protection against cybercrimes are by installing anti phishing software in user computers and devices, inducing biometric systems, registration

of internet devices, enhancing the websites security, DNS Scanning, deleting and blocking phishing in time and make guideline centers (Loganathan & Kirubakaran, 2011). Self reported cyber criminal behavior can be significantly predicted while using a variable and the predictor. Cybercrimes, especially the ID manipulation may not have worked as was predicted. A new validated way of measuring someone's anonymity on the internet should be devised. Anonymity is an individual difference which can interact with the level of anonymity obtained by situational factors (Baggili & Rogers, 2009).

Pakistanis are less attentive on cyber security issues. People are very busy in their routine lives. Only thevictims of the crime have taken some preventive measures in future regarding the cybercrimes.Only the IT field people are familiar with the tools to combat cyber-attacks. Regarding Pakistan's role in securing cyber space is worth noting at all. FIA and its regulatory bodies although have been performing well inmaintaining the laws. Some of the features in social networking websites should be banned in Pakistan. If we ban SNS, 90%of the cyber security issues will be resolved.It is recommended for parents of the teenagers to keep check on their children because this is the age of developing the habit ofmisuse of technology(Ahmed & Khan, 2015).

Both cyber pornography and sending messages to sex trading or trading sex on Internet are being listed among the top five cybercrime cases being registered every year. Manyof the criminals committed "Relations for Compensation" a communication for prostitution. Middle-aged men are giving money and expensive gifts toyoung girls specially students for sexual favors in return. Many criminals in Taiwan were caught by police for posting sexual offers with fake identities. The number of cyber criminals in Taiwan who acted independently has increasedfrom 43.8% in 1999 to 86.9% in 2004. A lot of criminals in Taiwan are male and the majority of them held a senior high school diplomas.

Disseminating messages about sex trading is the most frequently committed cybercrime amongundergraduate and graduate students (Lu, Jen, Chang, & Chou, 2006).

Introduction of different provisions in IT Act by the ITA, 2008 regarding the data protection are really vital and essential in the current business environment as several Indian companies handle large amounts of data that is being accessed or processed by their employees. The rising accountability of data handling persons or companies is necessary. The existing provisions and the additional or revised provisions under the ITA 2008 provide for criminal prosecution and stringent monetary penalties can be very effective against the cybercrimes. Absence of effective provisions to cope with the crimes like Cyber Stalkingisthe big loopholes in the act. It can be concluded that that whilst the ITA 2008 is still in the progress towards the implementation, it is surely headed in the right direction (Nappinai, 2010).

The preliminary research endorses a higher loss of the cost of cyber espionage and crime somewhere between 0.5% and 1% of the total national earnings for the United States. This is equal to be about $70 billion to $140 billion. A lower estimate is probably $20 billion to $25 billion. An awfully crude extrapolation could be to take this range for the US, which accounts for a little bit greater than a fifth of world's financial endeavor, and makes you up to $500 billion of international losses (Center for Strategic and International Stdies, 2013).

Working out on the behavior of cyber criminals and affects of cyber crimes on society will help find the means to overcome the drawback. Methods to overcome these crimes can broadly be labeled into three categories: Cyber legal guidelines (referred as Cyber laws), education and making policy. The entire approaches to manage cyber crimes either are having very less significant work or having nothing in a lot of countries. This lack of

work toughens the prevailing knowledge and it is needed to set new paradigms for controlling the cyber attacks (Saini, Rao, & Panda, 2012).

Hypothesis

H: More the time spent on social networking websites, more will be vulnerability for being a victim of cyber crime.

RESEARCH METHODOLOGY

Research design

Survey, Questionnaire and interviews weredesigned for the respondents. Students were surveyed through a questionnaire.Students of different universities across Pakistan who are users of social media websites and have social accounts were taken as universe of the study. Randomization technique was used. After randomly selecting four different universities; one from the each province, two main strata were defined; Male and Female students. From each university, four different departments were chosen randomly. Under graduate and post graduate students in equal number (25 each) were selected by at this stage. So a total number of 200 students from each university were selected. Total 800 (400 male and 400 female students) were taken as the sample from the sampling frame.

Testing Hypothesis

H_1: More the time spent on social networking websites, more will be vulnerability for being a victim of cyber crime.

$H1_0$:

There is no correlation between the time spent on cyber media and vulnerability for being a victim of cyber crimes.

Vol-X, Issue-II, Fall 2017
ISSN: 2070-2469
HEC RECOGNIZED
http://www.aiou.edu.pk/SAB/gmj/
Global Media Journal
Pakistan Edition

Regression

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.364[a]	.133	.132	.864

a. Predictors: (Constant), How often the social networking websites are being used

b. Dependent Variable: How often have the users been a victim or witness of cyber crimes

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	91.201	1	91.201	122.210	.000[a]
	Residual	595.519	798	.746		
	Total	686.720	799			

a. Predictors: (Constant), How often the social networking websites are being used

b. Dependent Variable: How often have the users been a victim or witness of cyber crimes

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	2.378	.067		35.356	.000
	How often the social networking websites are being used	.401	.036	.364	11.055	.000

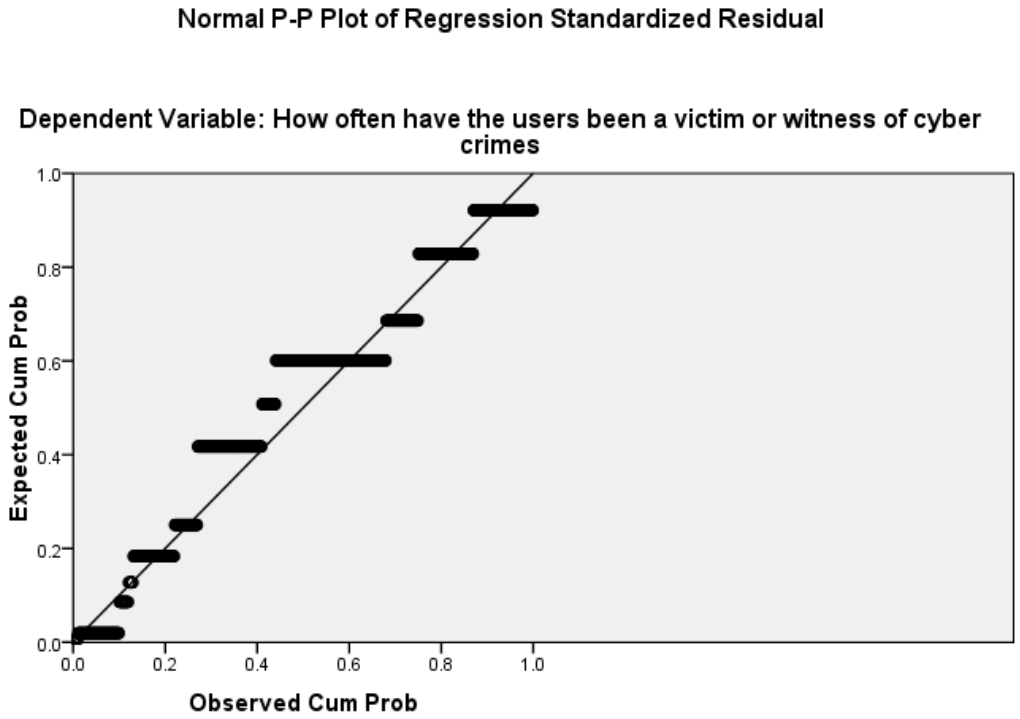
a. Dependent Variable: How often have the users been a victim or witness of cyber crimes

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2.78	3.98	3.04	.338	800
Residual	-2.180	1.221	.000	.863	800
Std. Predicted Value	-.772	2.792	.000	1.000	800
Std. Residual	-2.524	1.413	.000	.999	800

a. Dependent Variable: How often have the users been a victim or witness of cyber crimes

Vol-X, Issue-II, Fall 2017
ISSN: 2070-2469
HEC RECOGNIZED
http://www.aiou.edu.pk/SAB/gmj/
Global Media Journal
Pakistan Edition



Explanation

The R is the Coefficient of Correlation; the value that indicates what level of correlation between two or more variables/values exists and prediction becomes scientific. It is calculated by taking R-Squared. The value of R is recorded 0.364. R Square is the Coefficient of Determination and it calculates the measure of goodness of the fit which is recorded as 0.133. It is the proportionate measures of variance in dependant variable.

Thus on the basis of statistical inferences, the research concludes that there is a positive correlation between the independent and dependent variables as was hypothesized Null hypothesis is rejected and alternate hypothesis is accepted. The value of R^2 and Beta is fairly close to 1 (reference value: -1↔0↔+1) that proves a strong positive relation between independent and dependant variable. Significant values prove that there is 95% confidence level in predicting and generalizing the result over the whole

population.Overall the image reflects a strong positive correlation between independent and dependent variables.

Conclusion

On the basis of the research findings, it can be concluded that Pakistani youth who is obviously the biggest consumer of internet and cyber media has a very little awareness of different kind of cyber crimes and is vulnerable to be victim of cyber attacks. Criminals can easily exploit cyber media and social networking websites to cause harm to the people. Although some comprehensive laws such as PECO 2007 exist but strict implementation and regulation is highly desirable. Females and children are more vulnerable to be victimized by the criminals using cyber media. Freedom of expression over social media needs to be lined with social responsibility. Cybercrimes like pornography, hate-speech and blackmailing are causing severe negative impact on the society as a whole.

References

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

Baggili, I., & Rogers, M. (2009). Self-Reported Cyber Crime: An Analysis on the Effects of Anonymity and Pre-Employment Integrity. *International Journal of Cyber Criminology* , 550-565.

Bansal, D., Sofat, S., Harsha, S., & Saluja, S. (2011). Current Trends in Internet Usage and Cyber Crimes against Youth. *International Journal of Cyber Society and Education, IV* (1), 55-62.

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace.* England: Greenwood Publishing Group.

Center for Strategic and International Stdies. (2013). *The Economic Impact Of Cybercrime And Cyber Espionage.* Santa Clara: McAfee.

Chiu, D.-Y., Wang, C.-S., & Chung, T.-T. (2010). Attacking and defending perspective of e-Crime behavior and psychology: A systemic dynamic simulation approach. *JOURNAL OF SOFTWARE, V* (12), 1349-1354.

Dizard, W. (1997). *Old Media New Media: Mass Communications in the Information Age.* New York: Longman.

Halder, D., & Jaishankar, K. (2011). *Cybercrime and the Victimization of Women: Laws, Rights and Regulations.* Banglore: Information Science Reference.

Halder, D., & Jaishankar, K. (2013). Targeting teachers in the social networking sites: An analysis from legal and criminological perspectives. *SASCV 2013 Proceedings* (pp. 390-392). K Jaishankar.

Kolkata. *SASCV 2013 Proceedings* (pp. 378-382). K. Jaishankar.

Kosina, K. (2012). *Wargames in the Fifth Domain.* Vienna: Diiplomatische akademie wien.

Kumar, A. P. (2009). *Cyber Law; a view to social security.* Banglore: YFI & Anupa Kumar Patri.

Lu, C., Jen, W., Chang, W., & Chou, S. (2006). Cybercrime & Cybercriminals: An Overview of the Taiwan Experience. *Journal Of Computers, I* (6).

Maniscalchi, J. (2010, October 4). *The Human Impact of Cyber Crime*. Retrieved 12 14, 2015, from Digital Threat: http://www.digitalthreat.net/2010/10/the-human-impact-of-cyber-crime/

Manovich, L. (1999). *The Language of New Media.* Cambridge: The MIT Press.

Mambi, A. J. (2010). *ICT Law Book: A source book for information and communication technologies & cyber law in Tanzania & East African community.* Dar es Salaam, Tanzania: Mkuki na Nyota Publishers Ltd.

Nappinai, N. (2010). Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study. *International Journal of Commercial Law and Technology* , 22-28.

Servine, W., & Tankard, J. (2001). *Communication Theories: Origins, Methods and Uses in the Mass Media.* New York: Longman.

Sen, A. (2013). Linking Cyber Crime to the Social Media: A Case Study of Victims

Vol-X, Issue-II, Fall 2017
ISSN: 2070-2469
HEC RECOGNIZED
http://www.aiou.edu.pk/SAB/gmj/
Global Media Journal
Pakistan Edition

About the Author(s)

*** Asad Munir** is a Ph.D. Scholar at IUB Bahawalpur and a Research Associate with the Department of Mass Communication, Allama Iqbal Open University Islamabad.

**** Maryam Tahira Gondal** is a Ph.D. Scholar at IUB Bahawalpur.