Tsunami of Cyber Crime: Analysis of Cyber Crime New Trends, Causes and Remedies in Future Prospectus

Ahmed Mateen
Department of Computer Science,
University of Agriculture Faisalabad,
Pakistan

Qaiser Abbas
Department of Computer Science,
University of Agriculture Faisalabad,
Pakistan

ABSTRACT
The objective of this research paper is to bring forth the new challenges faced by Pakistan regarding the Cyber Crime. In this arena of technology, Pakistan is in the danger zone of Cyber Crime. Storm of Cyber Crime is hitting almost every country with new power and challenges**.** Like whatever other nation of the world, Cyber Crime is on ascend in Pakistan. A year ago, digital violations brought on an estimated misfortune adding up to $ 575 billion world over. This paper is divided into major three section. In the first section paper has discussed the new trends coming in Pakistan in future in cyber-crime. Section 2 discussed explains the causes of this storm of cyber-crime and in the 3rd section prospective solution/methodology regarding to check this problem.

Keywords
Cyber-crime, Hacktivism, IoT, Social Network, Cyber Forensic.

1. INTRODUCTION
Internet is a blessing in disguise but sometime this blessing change into curse due to the fever of cyber-crime .With the advent of the cloud Computing, all enter into the technology zone .And this technology zone is full of threat of cyber-crime. In this arena of technology, it often hear the words of Cyber Crime, Cyber War and Cyber Attack.

Identification of Cyber Crime is very difficult due to undefined and limitless Boundary. In Pakistan Cyber Crime victimization increasing day by day. The foundation of this wrong doing is the abuse of voice over Internet Protocol (VoIP).According to rating the abuse of VoIP in 2014 is five times more than the earlier year [1].

1.1 Cyber crimes in Pakistan
The rate of cybercrime in Pakistan is not precisely the principle world countries. Because web use in not as much far reaching. Lion's share of the populace dwell in rustic zones where the general population don't know about the innovation usage. A workshop washeld with ICT few year back which elaborated that "The temperament of digital wrong doing casualties to seek after cases is the significant obstacle in the method for examinations and activity against programmers and culprits in the nation". As indicated by him approximately 200 suit was accounted for in 2011 consider web miss representation, site hacking .The casualties don't document against the wrong doing in view of the apprehension of police, coercing and individual insider facts. There are bunches of wrong doings which have been given in the midst of the past years .Few year back FIA caught an item designer of an area establishment. The child was reprimanded for hacking social sites and Facebook IDs. He was used to force egg-producing through social web site accounts. The cybercrime department of of FIA caught a man who crippling messages and doing illegal activities with different govt departments. Similarly CIA caught some group which had executed infringement like Master card coercion in Italy. There are calculable amount of cybercrimes which happen in dayto day business.

1.2 Social behavior of peoples
The social web network is the crucial part in digital violations.. In social network one can without much of a stretch make false biography [2].The vicious normally make the fake biography of the famous people and alluring women[3].Men acknowledge the companion demand from ladies regardless of the fact that they are finished unknown [3].You can envision that it is so advantageous to right your casualty's data. There are suit like the vicious send away messages to the customer, cases to be old companion of them. He requests money related help guaranteeing that he is in the remote nation and has been a casualty of theft [3] The absence of mindfulness will make SNS clients turn into the casualty of deceitful. The pattern of online relational unions has turned out to be so normal these days. Individuals mingle themselves done these SNS. The lawbreakers plan young ladies and dramatic play with them. Knowledge get-together can without much of a stretch finished SNS [2]. Semantic role online networking like Facebook, twitter have been the root to assay possible reference [2]. SNS is likewise utilized for information [3]. Violent can undoubtedly speak with the broad people[3].There was a document created in 2010.Accordant to the document psychological oppressor target youngsters finished these SNS and online picture games[3].There was an instance of Irhabi fear based oppressor in few year back[3].He was accustomed to hacking sites and was instructing web hacker expertise to different Jihadis [3]. In Mexico city, as per a report created in 2009, misrepresentation drove is the main cybercrime. In USA Air power, there is sufficient individual data accessible in SNS for digital attacks [3].

1.3 Every new technology opens the door to new criminal approaches
Pakistan is trying to become the emerging country in the field of technology .Internet speed is double, bids for 3G and 4G and, funds for public sector in the field of Technology research is grand step towards the new horizon of Information Technology .But the lack of unawareness and proper legislation make the situation worse[3]. Cyber-crime is the one of the greatest dangers everywhere throughout the world. It is disturbing that because of unawareness rate of E-exploitation is expanding. E-Victimization is the sort of exploitation that is not happened vis-à-vis. It happened through PC or other electronic gadgets or programming. This may occurred to purposefully hurt the notoriety of casualty or gathering. Cybercriminal are comparable with conventional criminals [2]. In Pakistan many cyber laws are in waiting state .In this global technology era, there is a need of secure and

reliable cyber space environment. It is alarming situation that underdeveloped countries like Pakistan, cyber-crimes are on its peak.

2. LITERATURE REVIEW

In Pakistan, digital wrongdoings are new and confused curse. (Digital Crime) includes any criminal demonstration managing PCs and systems (Wired or remote) (Cyber-Crime). Because of absence of learning with respect to laws that location digital wrongdoings in Pakistan and casualties' rights a large portion of individuals don't answer to powers**[12].** Privacy and data theft will be the top security issues that organizations need to focus. Lived in this present reality where all data is in advanced structure. Person to person communication destinations give a space where clients feel protected as they collaborate with loved ones. On account of home clients, digital offenders would keep on targeting online networking destinations to take individual information [13].

3. MAJOR CAUSES BEHIND THE CYBER CRIME

3.1 Lack of law enforcement agencies in Pakistan

The working of Cyber law enforcement agencies in Pakistan is working in limited boundary. The concept of cyber-crime is different from the street crime so the tool and policy are must be different from the cyber-crime. Cyber attackers are faster than the cyber law maker.

3.2 Lack of new legislation

Older law does not adequately addresses the difficulties of digital wrongdoing subsequently criminal did not get appropriate discipline in Pakistan. As per a media report, more than 10,000 cybercrime cases are pending in Pakistan while 250 affirmed guilty parties has been without set in light of wasteful law[7]. Pakistan just has a dead digital wrongdoings law in type of "Digital Crimes law" that was last overhauled in 2009. A lasting law is need of great importance and with presentation of 3G innovation around the bend, this law turns out to be even a more prominent need [1].

3.3 Lack of cyber forensic

PC criminology (once in a while known as PC measurable science is a branch of computerized criminological science relating to legitimate proof found in PCs and computerized stockpiling media[8]. The foundation of Punjab Forensic Science Agency in Punjab checks new period in our national history. In Pakistan many cyber-crime is pending due to unavailability of the forensic lab. Proper digital evidence is required due to the complicated nature of the crime.

3.4 Scarcity of the skilled cyber crime fighter

Cyber security Professional are not available in Pakistan .In future there is a need of Cyber army to control the war of cyber-crime. Pakistan have not well renowned educational institute to produce the professional in this field Therefore, all have a shortage of skilled labor in this area.

3.5 Lack of cyber crime curricula

One of the reason of lack of awareness about the cyber-crime is the poorly define Cyber Crime Curricula. There is no cyber-crime curriculum in the course outline of BS and M.Sc. programs even in the renowned IT universities in Pakistan.

3.6 Fail to report

In Pakistan Victim try not to report against the digital wrongdoing in light of the apprehension of police, coercing and individual secret. Some organization also do not inform about the cyber-crime incident due to reputation of the firm.

3.7 Negligence in the use of technology

Society is not by any means arranged for the 2G innovation yet since individuals don't know how to shield their cell telephones from getting hacked [1]. There is not a good sense of technology in Pakistani society. Zeal of technology is lost due to the lack of awareness. Karachi police has as of now uncovered that Skype, What's App and Viber are being utilized for violations today. Individuals are moving from Wi-Fi /DSL system to 3G based virtual worlds and not at all like DSL associations, identifying the area of a 3G association is moderately troublesome and that is the reason it can be utilized for kidnappings in the end [1].

3.8 Youngster's obsession

In Pakistan youngsters are obsessed with the use of Internet .They some tine do cyber-crimes for the sake of enjoyment. Unemployment also plays a motivated role in this context .People want to earn money in short time .So they use latest technology for their criminal purpose.

3.9 Mental illness

Disorder in the culture can create different dysfunctional attitude in Society .Mental ill people cannot control their thoughts and emotion. Pakistani culture is facing many up and downs now a days.

3.10 Lack of evidence

This is a big challenge for the law enforcement agencies to collect digital evidence for the cyber-crime .In Pakistan there is not any recognized forensic lab for this purpose. Govt. should take notice and open new lab in this regard as soon as possible to tackle the Cyber war.

4. NEW TRENDS IN CYBER CRIME

4.1 Mobile Apps

Security Predictions for 2012 is that Smartphone's and tablets will continue to be targets for cybercriminal attacks[4].The velocity of Mobile Apps cyber-crime is increasing especially in the mobile banking apps .

4.2 Cyber terrorism

Cyber Terrorism is spreading like wild fire all over the world. IN underdeveloped countries like Pakistan terrorist organization aligns with cyber-crime specialist to do illegal activity. These cyber-crime criminal are also funded by national and international terrorist organization. There is Cyber war between India and Pakistan which makes the situation worse.

4.3 Hacktivism

Hacktivism is the demonstration of hacking, or breaking into a PC framework, for a politically or socially spurred reason. The person who plays out a demonstration of Hacktivism is said to be a hacktivist [5].Using the internet media for Hacktivism is in peak in Pakistan. DNS seizing is a basic issue in such manner. DNS seizing (now and again alluded to as DNS redirection) is a sort of vindictive assault that abrogates a PC's TCP/IP settings to point it at a rebel DNS server, in this way negating the default DNS settings [14].

4.4 Pornography

Pornography is the 'representation of sexual movement in print or on film to invigorate sensual instead of stylish or passionate sentiments.

4.5 Social Media crimes/Cyber stalking

The use of social media is increasing day by day in Pakistan. Many Women are black mail and harassed through the social media Even their families are also disturbed. Young girls are also attacked due to the unawareness of the cyber-crime and they also do not know about the laws which protect and safe then from this epidemic Cyber disease. In Pakistan many divorce are occurring due to this Cyber blackmailing. Defacement is common through social media.

5. PROACTIVE MEASURE OR METHODOLOGIES

5.1 Awareness campaign

Awareness campaign should be launch in different organization especially in educational institution to train the youth. Society contribution is necessary for the successful campaign. Seminar should also conduct to educate masses for this critical issue.

5.2 Ethical hacker / Cyber fighter

A moral programmer is a PC and systems administration master who methodically endeavors to enter a PC framework or system for its proprietors with the end goal of discovering security vulnerabilities that a noxious programmer could possibly abuse [11]. To fight with cyber-criminal, there is a need Ethical fighter or Cyber fighter army. He has to introduce new training programs for producing ethical hackers.

In this graph to explain the cyber crime summery of diff rent year. Every year the trends of cyber crime increase day by day .Because no rules or regulation clearly define for this crime.

5.3 Curricula development

Cyber Crime Curricula should be developed form higher level .HEC (Higher Education Commission) should take notice and include the syllabus of cyber security in broader prospectus. These projects range from particular tracks inside customary scholastic projects to specific degree titles grew exclusively with the end goal of delivering digital competent graduates [10].

5.4 New legislation

There is a need comprehensive security legislation to deal with the emerging technologies. [9] National Response Center is remarkable step in this regard. Old law cannot be implemented in true way .In Pakistan new. In Pakistan, radical exercises are done on online networking to aggravate and disturb the power, uprightness and believable of people and establishments, this requests escalated enactment against digital fanaticism and fear based oppression and its linkage with global group battling in war against psychological warfare. (Kundi et al. 2012; Bell, 2002). New cyber law should be implemented to tackle the problem of the new technologies.

5.5 Women awareness cell

Special awareness cell should be created for women awareness about cyber-crime and cyber law. Women in Pakistan require special awareness about the cyber-crime because woman victimization through cyber-crime is increasing day by day .Black mailing through social media for example through face book is hitting like storm. They even cannot report about the incident to their families .Special counseling is required in this matter. Special Cyber Crises cell should be maintained especially for Women.

In this diagram to explained that the new trends or terminological apply for this act .Different methods apply for achieve these targets, like that Dos attack are most popular in cuber crime.

6. RESULTS

The main target is the people who were teen agers, a study narrate 90% of people is aware about those threats while 10% of the people are not know that with those cybercrimes. But in this scenario the age was not effect or matter in this case all depends about your nature and thinking. In Pakistan 55% people are used the social sites via a internet most of the population think that it is threat while some narrate it crime.

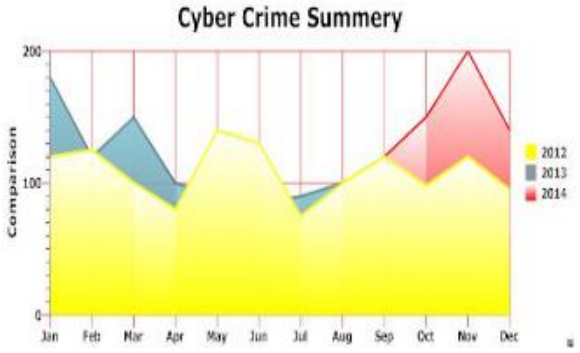

Fig. 1: Shows the summary of cyber- crime

Table 1. Cyber-crime summery data

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2012	120	125	100	80	140	130	75	100	120	98	120	95
2013	180	120	150	100	90	85	90	100	80	85	100	90
2014	80	78	80	75	50	60	67	100	120	150	200	140

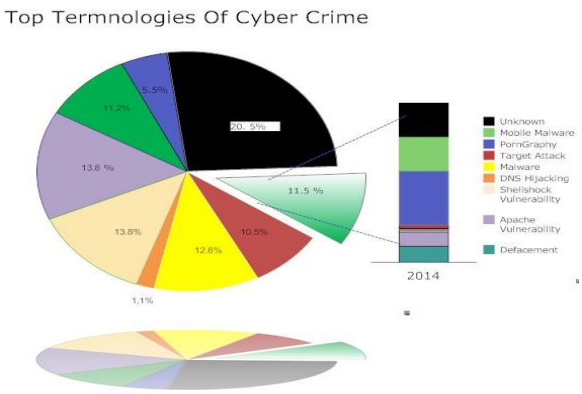

Fig. 2: Shows that the terminology of Cyber Crime.

Table 2. data of cyber crime terminology

Attacks	Unknown	Mobile Malware	DNS	Malware	Target Attacks	Defes-ment	Wilner-ability	Pornography
Ratio	20.5%	11.2%	1.1%	12.0%	13.5%	11.5%	9.2%	5.5%

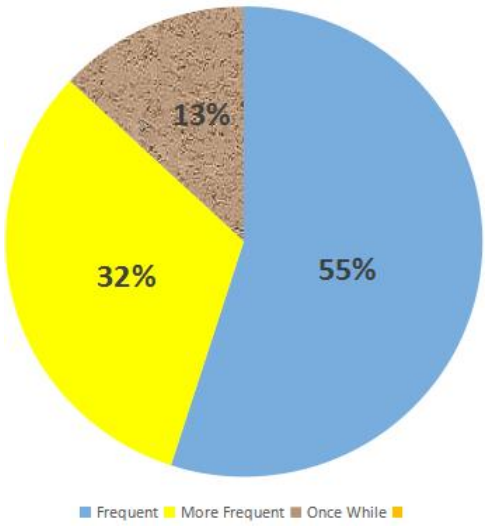

Fig. 3. Internet usage detail.

In above diagram to explain that the usage of internet in daily life the people use the internet for differences ways.

Table 3: usage of internet

Frequent	55%
More Frequent	32%
Once While	13%

7. CONCLUSION AND FURTURE WORK

People are not aware the true use of technology. This Lack of awareness gives birth new cyber-crime. while finish up the examination by specifying that in Pakistan individuals are less mindful on digital security. Individuals are occupied in their everyday schedule. Just those individuals who have been the casualty of the wrongdoing have taken some preventive measures. There is a huge responsibility on the shoulder of government and educational institution to work together to eliminate this curse .Cyber-crime laws should be proper implemented. Cyber law agencies should be active to combat the problem of cyber-crime in near future.

In the future the cyber-crime is the most popular crime category, since the different technical advancements have caused the societies to gradually become "e societies". So hope that technical change of the past 20 years which gave birth to cyber-crime, will find the way to fight this new crime type.

8. REFERENCES

[1] Andel, T. R. and McDonald, J. T., 2013. A Systems Approach to Cyber Assurance Education. In Proceedings of the InfoSecCD'13: Information Security Curriculum Development Conference .

[2] Avais, M. A., Wassan, A. A., Narejo, H., and Khan, J.A., 2014. Awareness Regarding Cyber Victimization among Students of University of Sindh, Jamshoro. International Journal of Asian Social Science. 4(5): 632-641.

[3] Bhadauria, S. S., Sharma, V., and Litoriya, R., 2010. Empirical analysis of Ethical issues in the era of future information technology. InSoftware Technology and Engineering (ICSTE) 2nd International Conference on 7(2): 2-31.

[4] Gunjan, V. K., Kumar, A., and Avdhanam, S., 2013. A survey of cyber crime in India. In Advanced Computing Technologies (ICACT), 15th International Conference on: 1-6.

[5] Harris, J., 2004. Maintaining ethical standards for a computer security curriculum. In Proceedings of the 1st annual conference on Information security curriculum development, 5(6): 46-48 .

[6] Holt, T. J., and Bossler, A. M., 2014. An assessment of the current state of cybercrime scholarship. Deviant Behavior, 35(1): 20-40.

[7] Hooper, C., Martini, B., and Choo, K. K. R., 2013. Cloud computing and its implications for cybercrime investigations in Australia. Computer Law & Security Review, 29(2): 152-163.

[8] Jadhav, D. S., Parode, V. D., Dige, Y. C. and Patil, S. K., 2013. Virtual offense in Maharashtra (India): Legend and truth?. In Intelligent Systems and Signal Processing (ISSP), International Conference on . 319-324.

[9] Jamil, D. and Khan, M. N. A., 2011. Is ethical hacking ethical?.International Journal of Engineering Science and Technology (IJEST), ISSN, 0975-5462.

[10] Kundi, G. M., Nawaz, A., Akhtar, R., and MPhil Student, I. E. R., 2014. Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. Journal of Information Engineering and Applications, 4(4): 61, 71, 2225-0506.

[11] Luallen, M. E., and Labruyere, J. P., 2013. Developing a critical infrastructure and control systems cybersecurity curriculum. In System Sciences (HICSS) 46th Hawaii International Conference on, 1782-1791 .

[12] Papanikolaou, A., Vlachos, V., Papathanasiou, A., Chaikalis, K., Dimou, M., and Karadimou, M., 2013. Cyber crime in Greece: How bad is it?. In Telecommunications Forum (TELFOR). 1-4.

[13] Ramesh, P., and Maheswari, D., 2012. Survey of cyber crime activities and preventivemeasures. In Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology 6(4): 301-305 .

[14] Razzaq, A., Hur, A., Ahmad, H., and Masood, M., 2013 . Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In Autonomous Decentralized Systems (ISADS), Eleventh International Symposium on. 1-6.

[15] Patki, A. B. Lakshminarayanan, S. Sivasubramanian, S. and Sarma, S.S., 2003. Cyber crime information system for cybernetics awareness. I. Proceedings.2003 International Conference on. 46-53.