A Critical Study Of Cyber Crimes And Cyber Security In Khyber Pakhtunkhwa

Nadia Noreen1, Kokab Saeed2, Alam Zeb Khan3, Muzamil Shah4, Hidayat Ur Rehman5, Aliya Mahnoor6

1Assistant Professor, Department of Law Hazara University Mansehra
2Assistant Professor Department of Law Hazara University Mansehra
3Assistant Professor School of Law Quaid-i- Azam University Islamabad
4PhD Scholar
5Assistant Professor Department of Law AWKUM
6LLM Scholar

ABSTRACT
This research article attempts to explore and review the progress of Cybercrime and cyber security in Khyber Pakhtunkhwa. The main purpose of the article is to examine the reasons of increase of cybercrime in society has amplified by usage of internet. Because of lack of training of preventive measures people are exposed more to the risk of cybercrime which include hacking, spamming and harassment. All these offences are discussed in details and then the article suggests how to avoid them. Primary data is collected from the national Response Centre for cybercrime. Survey in among the students of the University of Hazara was also conducted to analyze the trend of victimization among the students and correlation between genders.

KEYWORDS: Cyber Crimes, Cyber Security, Online Harassment, Hacking, Online theft,

INTRODUCTION
Considering the development of technology one of the most cutting-edge technologies that is well-known worldwide is the internet. The number of people using the internet has climbed from sixteen million in the 1990s to over three billion in 2021. The internet is regarded as being an incredibly important component of any man's existence.
Before the internet was invented people used to keep all the records in the form of hardcopy. Then the idea of internet in the 60's came. Paul Baran and Donald davies were the owners of this idea. World Wide Web launch changed the dimensions of internet. It is abbreviated as WWW and it was launched in 90's. This increased the users of internet day by day. After the invention of computers, smartphones were invented. Smartphone that easily fits in our pocket gathers more attention and connectivity than the computers. Computers can be used in a positive way as well as in a negative way. It can be used to harm other through cybercrime. If something has a positive side it has a darker side too. People often don't know about cybercrime and what are its affect. We can say, in simplest words, that cybercrime is a crime which is committed through a computer having accesses to internet. Frauds, impersonating stealing someone’s identity, pornography, and theft of intellectual property are included in it. It is a highly growing and sophisticated kind of theft in the contemporary world.¹

Due to this rampant increase in cyber crimes the UN General Assembly passed the resolution 55/66 on 4th December 2000 to ensure that states must safeguard their laws against criminal misuse of information technologies. The privacy, integrity and provision of data and computer systems must be saved from abuse.

Before this research article proceeds further, certain terms need to be explained for the convenience of the readers.

**Cybercrime**—*Meaning of*

An activity in which computer or internet is used as an instrument to do an illegal thing" For example: stealing people’s identities, committing fraud, disturbing someone’s privacy. Traditional crimes are also included in it. For example hacking someone’s email, frauds related to credit cards, etc.

**Cyber Security**—*Meaning of*

Its being protected by internet-connected systems, including hardware, software and data, from cyber-attacks In a computing context, security comprises cyber security and physical security both are used by enterprises to safe against unauthorized access to data centre and other computerized systems. The security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security².

**Need of cyber security**

The range of operations of cyber security involves protecting information and systems from major cyber threats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people. Some of the common threats are:

- **Cyber terrorism** It is the innovative use of information technology by terrorist groups to further their political agenda. It took the form of attacks on networks, computer systems and telecommunication infrastructures.

- **Cyber warfare** It involves nation-states using information technology to go through something another nation's networks to cause damage. In the U.S. and many other people live in a society, cyber warfare has been acknowledged as the fifth domain of warfare. Cyber warfare attacks are primarily executed by hackers who are well-trained in use of benefit the quality of details computer networks, and operate under the favourable and support of nation-states. Rather than closing a target's key networks, a cyber-warfare attack may force to put into a situation into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce⁴.

- **Cyber espionage** It is the practice of using information technology to obtain secret information without permission from its owners or holders. It is the most often used to gain strategic, economic, military advantage, and is conducted using cracking techniques and malware.

**Cyber Criminals**
The word Cybercriminals refers the individuals who commit cyber crimes. They can be categorized into three groups that reflect their motivation.

**Cybercriminals Hungry for recognition**
- Hobby hackers;
- IT professionals (social engineering is one of the biggest threat);
- Politically motivated hackers;
- Terrorist organizations.

**Cybercriminals - not interested in recognition**
- Psychological prevents;
- Financially motivated hackers (corporate espionage);

- State-sponsored hacking (national espionage, sabotage);
- Organized criminals.

**Cybercriminals - the insiders**
- Former employees seeking revenge;
- Competing companies using employees to gain economic advantage through damage and/or theft.

Factors behind Cyber Crimes
Different types of crimes are committed for different reasons which can be elaborated as under:

**Reasons behind online harassment of women**
- Psychological reasons like loneliness, insecurity lack of family support.
- Less knowledge of computers
- Lack of awareness about cybercrime
- The reason for greater victimization of women is that the social context of Pakistan allows for suppression of the female voice. Because of the concept of "Honour" many women victimization cases are swept under the carpet.

**Online Purchasing Hacks**
In Khyber Pakhtunkhwa the occurrence of crime through mobile and internet are ranked on no.3. Survey of study of online purchasing in Khyber Pakhtunkhwa results in that people are not comfortable in online paying method like through credit card they worried about their online transaction.

**Percentage of Cybercrime in Khyber Pakhtunkhwa**
1. System damage is about 7%.
2. Illegal access to computer is about 6%.
3. Risk of interception of computer data is about 5%.
4. Trade mark offences are about 1%.
5. Controlling sending of spam is about 2%.
6. Computer related acts including hate material are about 15%.
7. Privacy and data protection measures are about 7%.

Identity offences related to computer are about 17%.

**Individuals ranking their experiences**
8. A survey was also made among the students to rank their experiences according to various cybercrimes such as spamming, hacking, phishing, harassment and stalking etc. Students were asked to rank their experiences between 1 to 10 according to the seriousness of the crime. Three categories were made;
- Very serious which were ranked above
- Moderate which were ranked between 4 to 7
- Non serious which were ranked below 4.

<table>
<thead>
<tr>
<th>Category</th>
<th>Gender</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very serious</td>
<td>Women</td>
<td>43.3%</td>
</tr>
<tr>
<td>Serious</td>
<td>Women</td>
<td>62.9</td>
</tr>
<tr>
<td>Moderate</td>
<td>Women</td>
<td>1%</td>
</tr>
</tbody>
</table>

In response to these following actions are taken like Serious action here represents the reporting of case to the police or if not solved by the police than to the FIA. The non-serious actions here represents the reporting of crime on social media application. After this survey we get to know that whatever the category is whether serious or non-serious some sort of action must take place by the victim.

To earn a huge amount of money, Cybercriminals always choose an easy way. Banks, casinos, companies, and, financial firms are the prosperous organizations and their target centers where an enormous amount of money runs daily and has diplomatic information. It’s very difficult to catch those criminals. Hence, the number of cyber-crimes are increasing day-by-day across the globe. We required so many laws to protect and safeguard them against cyber-criminals since the computer is vulnerable. We have listed some of the reasons:

- Easy to access computers – Since technology is complex, it has become very difficult to protect the computer from viruses and hackers. There are so many possibilities of hacking when we safeguard a computer system from unauthorized access. Hackers can steal access codes, retinal images, advanced voice recorders, etc that can mislead the biometric systems easily and can be utilized to get past many security systems by avoiding firewalls.
- Capacity to store data in comparatively small space.
- The computer has a unique characteristic of storing data in a very small space. This allows for much easier access or removal of information through either physical or virtual media.
- Size to store computer data in comparatively small space – The computer has got a distinctive feature of storing data in a very small space. Due to this, the people can steal data very easily from any other storage and are using this for their purpose.

- Complexity of Code – The computers can run on operating systems and these operating systems are programmed with millions of codes. There may have mistakes in the code. The human brain is defective so that they can commit mistakes at any stage. The cyber-criminals take advantage of these gaps.

- Negligence of the user – Human beings always neglect things. So, if we make any negligence in protecting our computer system which leads the cyber-criminal to the access and control over the computer system.

- Loss of evidence – The criminals can easily erase the data which is related to the crime. So, Loss of evidence has turned into a very usual evident problem that disables the system beyond the investigation of cyber-crime

### Conclusion and Recommendations

The study indicated that in one way or the other, cybercrimes are silently present and pose a threat to the developed and developing countries. The instances of cybercrimes are not reported rather discussed socially; on the other hand the perpetrators are invisible under the cyber world.

KPK should adopt the proper laws and procedures of anti cyber crimes effectively. On the other hand it has been proven that it is the responsibility of the individual to protect his/her own Internet connection. It could therefore be suggested that Governments and local authorities including Police and Education Services should work more closely with the Internet Service Providers to protect minors on the Internet. Despite all the developments in the domain of Child Protection Software, young people will always find a way of avoiding a protective firewall. Therefore education would serve an important role in protecting children. Furthermore if the culprits are identified law enforcers could punish and remove the criminals’ access to the internet.

The guard off the cyber-crime effectively, it needs to set up multidimensional public-private collaborations between law enforcement organizations, the information technology industry, information security organizations, internet companies, and financial institutions. A far apart from the real world, Cyber-criminals do not combat one another for predominance or authority. Rather, they do their tasks together to enhance their abilities and even can help out each other with new opportunities. Therefore, the regular ways of fighting the crime cannot be used against these cyber-criminals.

### References

https://www.satp.org/potential-threat/cyber-crimes/pakistan-khyberpakhtunkhwa-khyberpakhtunkhwa#


http://dx.doi.org/10.31703/gpr.2019(IV-II).02