Cyber Crime: Threat to Society

Asst. Prof. Ms. Shambhavi Yashwant. Tendolkar

B.Sc(Mathematics)LL.B. LL.M.

Victor Dantas Law College, Kudal

Introduction:

India has always been referred to as a developing nation but as the technological advancements are taking hype our country is nowhere behind in the race. Internet access has become anybody's cup of tea so also anything that human wishes to fetch can look for on the internet.

Where there is human there definitely is crime present. But are there really any crimes related to the cyber web. Can a knowledge providing handle be this risky or scary when it comes to the safety and protection of the users?

In the early 90's the resources were not at that strength that it would lead to a direct commission of any particular crime, but as this web have gotten a massive spread, the range of commission of the crimes has also raised.

There are no any gender oriented victims, males females at a particular strain are all getting affected by the cyber-crimes. Also the flow chart if created any will always have an extra column to add a new cyber-crime to the list. Human brain really can't be challenged when it comes to having a new and improved version of anything that also includes crimes and offences for those matter cyber-crimes. Every other minute a person is getting fished, bugged, hacked or being a victim of such a cyber-threat new to that person and new to the whole cyber system itself.

Where there is a problem there is a solution. But are these solutions enough to deal with the current situation? Is what the matter to be scrutinized. Being sceptical about this issue I personally feel that the ratio of the crimes is increasing day by day and it's high time to consider this newly emerged threat and try to curb the issue as early as possible.

The following points will help to understand the point in detail.

What do you mean by cybercrime?

An offence committed by the means of computer or cell phone or any device devise, technologically advanced, fully equipped and also having internet support. But is it only the basic requirement to commit the offence? No!! It's not any basic device is also useful and can be used to commit an equally grave of an offence.

Cyber-crime-an expanded definition.

Any such activity or an act that leads to sexual assault, phishing, hacking, virus, bugs, including threats to people any other devices via any single or multiple devises is all covered under the cyber-crime.

Sharing, sending, broadcasting any illicit, obscene image, videography, photograph, recording without the consent of the receiving party, with pure men's rea, which further leads to not just degrading the modesty of women but all the genders available and to the society at large?

Bugging, phishing is associated with the type of hacking like money or account of the devise holder or accountholder. Mostly these bugs are designed to act as viruses and corrupt the data of the other devise to which it is transmitted. N number of styles can be formulated to develop such viruses and bugs to create a chaotic situation.

It's not safe to say that highly secured data and devises don't get bugged, it's a technological advancement and any particular system can get destroyed within seconds by accessing such corrupt data or bugs.

Our nation is getting highly digitalized in every other minute on the clock to be literal. After demonetization as an up gradation new improved and high-tech systems of money transfers were introduced to the public for safe any easy transfer of money referred to with the popular name "cashless transaction". It's again not any secured and safe method compared to our old-school pattern of hard cash dealings. Also, the banking servers are not always a good friend and that leads to chaotic situation sometimes, which you never know can turn into offence.

Other kinds of offences that are associated with the cyber crime are copying of any data which is uncensored or on permitted. Causing a threat to the government and nation by utilizing all the available methods to put the highly important data into unsecured and share with all mode that can lead to big of a dangerous situation for nation as whole.

Who can be referred to as offenders or cyber-criminals?

The answer is really very easy. Any person who commits any of the acts from the above provided list can be called a cybercriminal. Widely this term is referred to a person who is efficient at using his tech skills to do all malicious and illegal activities. Not any particular individual joint-offenders, collective criminal intention holders are all incorporated under the scope.

Trading illegal content online or scammers, drug dealers are all a part of cyber-criminals.

Some cyber-criminals are

1. Black hat hackers
2. Cyber-stalkers
3. Cyber terrorists
4. Scammers etc.……[1]

How are cyber-crimes actually committed?

These offenders target the vulnerable areas in the tech region. Mostly low-quality data protection un secured transactions are the major reason for falling prey to such cyber-attacks. Easy to hack and destroy is the key to such offences.

Sexual assaults like sexting, trolling, pornographic data sharing and more such acts are also increasing due to the ease of technological advancements to reach the society at large.

In reality if we be skeptical to seek the reason behind commission of such offences the intention and criminal mind has just got a new platform. To put it in much easier way the thought hasn't changed just the mode and method got "updated".

Why do these cyber-crimes happen?

To be precise the reason is not much different from the regular commission of crimes, those same regular ways of thinking and reasons can be associated with this field of offences. A little to add, power or pleasure of having skills that can be destrucutfull can be an addition.

When do such acts become offence?

All the acts done in the circumscribing limits of law are legal. So also, hacking or related activities are non-offenceful if are done with legal validification or if fall under exceptions.

[1] https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention

Oftenly to find the real offender or to fetch what is illegal, illegal becomes legal. But then again, all the information data, received is to kept secret or shall not be used for personal or any other purpose but legal.

Are cyber-crimes such a big threat to society?

Oh yes!! Because the rate of speed at which the nation or even the whole world Is getting digitalized is so high, we definitely need to work on protection and safety from such cyber threats. As the necessary information is saved in the form of soft data it is not much of a task to convert, delete or consume such data. Why and how this data if received can be used is really not though to think about but unimaginable.

All the government related information; data related to forces, security of nation and all the citizens of course needs to be secured.

Unfortunately, this kind of threat is invisible and preplan or backups are the only option. Not falling prey to such crimes is only in the hands of users.

Denying the access to unknown sites, messages, or contacts also not sharing personal and important information, being smart and careful enough to understand the threat are some of the ways to save yourself from getting victimized at the hands of the cyber-criminals.

What are the legal resources available for such cyber-crimes?

1. The Information and Technology Act, 2000 does provide a wide range of options and provisions as to protect the people from such crimes and give them justice. Multiple sections talk on various strains of the crime and what exactly the Act is in favor of is all clear in the name itself.
2. The Indian Penal Code also has made various provisions for such activities. The 2013 amendment Act introduced some this generation crimes making to list of crime against women which are a part of cyber-crimes. Penalties are also made severe to teach such criminals a good lesson and try to reduce and stop such offences from getting repeated.
3. Cyber cells are established as one stop service providers for all the victims of all types of cyber-crimes. It’s really a smart move to have a separate cell as skilled people can easily find a hack against such hacks and crimes, which also will reduce the burden from the other bodies like police stations.
4. Various advertisements are also displayed and broadcasted for the regular public awareness.

List of various Cyber offences.

1. Money laundering
2. Hacking
3. Phishing
4. Scams
5. Identity theft crisis
6. Ransomware attacks
7. Internet fraud[2]

The above list is all related to data scams, fake accounts, messages, fraud by using personal information, non-encryption and other such activities.

Other cyber-crimes

1. Trolling
2. Stalking
3. Cyber bullying
4. Piracy
5. Social media scams
6. General recruitment frauds
7. Extortion
8. Drugs and other related scams etc.

Safety measures to prevent cyber-crimes.

a. Be sure with an up-to-date security like antivirus.
b. Never trust or browse the unsolicited and unknown sites.
c. Do not download any unknown files, attachments, etc.
d. Utilizing suitable and safe passcodes/ passwords.
e. Always protecting the data in any way possible from such threats.

Cyber-crimes are absolutely not unknown now. The speed of the tech popularity is somewhere directly proportional to defaming the same for all the various crimes attached.

[2] https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention