Issues and Challenges to Control Cyber Crimes in India

Dr. Monika Mishra*

Assistant Professor, Apex School of Law, Apex University, Jaipur-303002 (Rajasthan)

Abstract - The purpose of this study is to make an attempt to explore the problems and difficulties that are associated with cyber crime in India from an ethical point of view. The study of morality, or ethics, is a subfield of philosophy that examines questions such as "what constitutes appropriate behaviour?" The fields of corporate ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics have all seen an increase in the number of ethics centres and programmes dedicated to the study of ethics. It is becoming increasingly clear that cybercrime poses a significant risk. There are several reasons why computer technology is considered to be one of the most essential general purpose technologies in this day and age. In today's day and age, it is utilised by practically all of the businesses, establishments, and people. Computer technology makes life so much quicker and more efficient, but it also exposes people to a new kind of crime known as "Cybercrime," which is one of the most dangerous types of criminal activity. Cybercrime is a type of offence that deals with the cyber world and encompasses computer security, information security, and mobile security as well. The development of information technology provides a lot of benefits to us, but it also brings a lot of issues and obstacles. Everyone is becoming increasingly interested in cybercrime as a result of the growing number of offences committed in the world of information technology.

Keywords - Cyber Crime, Issues and Challenges in India, Computer Security

---------------------------------x--------------------------------

1. INTRODUCTION

The study of morality, sometimes known as ethics, is a subfield of philosophy that examines the nature of good and evil. There has been a proliferation of ethics centres and programmes that focus on areas such as corporate ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics. A significant risk is being posed by the rise of cybercrime. The term "cybercrime" is used to refer to a broad category of criminal activity in which computers or computer networks are used as a tool, a target, or a place of criminal activity. Examples of cybercrime range from "electronic cracking" to "denial of service attacks," and include a wide range of illegal activities. It is also used to cover more traditional types of criminal activities in which computers or networks are utilised to facilitate the illegal activity. Cybercrime has the potential to halt any railway, regardless of its location; it may also cause planes in flight to be misguided by sending them the wrong signals; it may result in sensitive military information being obtained by unfriendly nations; it may also halt electronic media; and it may cause every system to fail in a matter of seconds. [1]

It is the purpose of this research to examine some of the elements, effects, and future possibilities of this cyber technology, with particular regard to India's Cybercrime threat. In India, efforts have been undertaken to examine the legal structure that may be used to regulate it. For starters, the concept of 'crime' must be defined in terms of its scope. As a result, it is clear that "crime" is a relative Phenomenon, universal in nature, and that it has been observable in almost every society from ancient times to the present. All societies have their own set of definitions for what constitutes criminal behaviour and conduct that is punished by law, and this has always been shaped by the religious, social, political, and economic values prevalent in the culture in question. As a result, 'penal liability' conduct has always been impacted and characterised by the overall outcome of these criteria from their inception. Parallel to this shift in crime's definition, the types of criminals who commit it have also evolved in response to the rise of information technology. The notion of crime in Indian civilization, particularly in the ancient period, was heavily influenced by religious interpretation. The time was characterised by a total absence of religious influence. It is widely believed that all political and social actions, including the infamous "crime," are the result of supernatural forces at work. [2]

1.1 Cyber crime

An act of criminality is considered cybercrime if it is carried out primarily via the use of a computer. According to the Department of Justice, the term "cybercrime" now includes any criminal behaviour including the storing of evidence on a computer. It is becoming increasingly difficult for people and governments to deal with cybercrimes that have been made feasible by computers, such as network intrusions and the spread of viruses, as well as computer-based versions of existing crimes such as identity theft. Typically, cybercrime is described as a crime performed utilising a computer and the internet to steal a person's identity, sell illegal goods, stalk victims, or disrupt operations via malicious software. With the rapid advancement of technology, it is just a matter of time until cybercrime rises in frequency and severity. [3]

1.2 Types of Cyber Crimes

The following is a list of the numerous sorts of online criminal activity that are expressly specified in the Information Technology Act of 2000:

i. Tampering with computer source documents:

The process of purposefully concealing, destroying, or altering any computer source code that is utilised for a computer, computer programme, computer system, or computer network where the computer source code is required by law to be retained or maintained in its original form. In the case of Cox v. Riley, which took place in the United Kingdom, an irate worker purposefully erased a computer programme from a plastic card that controlled a computerised saw, with the intention of rendering the saw useless. In his investigation, Stephen Brown LJ discovered that the card had, in fact, been harmed; as a result, its utility has been lost, and it would require both time and money to rectify the problem.

ii. Hacking with computer system:

A hacker is someone who finds ways to circumvent a system's security measures in order to obtain unauthorised access to the system. There are a number of ways to accomplish this, including by stealing, guessing, or otherwise deceiving the software that checks for a password. You have Donald Gene Burleson to thank for that, of course. Texas8 Burleson, a senior programmer/analyst, was fired by his employer, USPA. As a USPA computer operator, he had access to the system's user names and passwords. In order to exact his vengeance, he wrote a software that erased crucial data from the systems and forced a four-hour shutdown of the whole network. In the end, he was found guilty of damaging and hacking into the company's computer network.

iii. Publishing of information which is obscene in electronic form:

It is a term that refers to the act of publishing or transmitting in electronic form any anything that is considered to be offensive. The classic case of United States v. Thomas (1996)10 included a defendant who operated a website through which users could download pornographic images onto their personal computers and even place orders for pornographic DVDs that were sent to their homes. It was determined that he was responsible for transmitting offensive content in public spaces when doing so was forbidden.

iv. Protected System:

Anyone who gains access to a protected system without authorization or makes an effort to get access to such a system is subject to the possibility of being fined and imprisoned for a period that might last up to 10 years, depending on the severity of the crime. Because virtually all of the Certifying Authority sites will be drivers of commerce, the government has the authority to proclaim almost all of these sites to be protected. This is because all of these sites are vital to the nation.

v. Breach of confidentiality and privacy:

A violation of the Information Technology Act occurs whenever someone gains unauthorised access to a person's electronic records or documents, or if that person reveals that person's electronic records or documents to a third party without that person's authorization or knowledge. In McGregor vs. Procurator Fiscal of Kilmarnock14, a concerned neighbour of a police officer asked the officer to look into the guy with whom his 18-year-old daughter was living. Both the Police National Computer and the Scottish Criminal Records Computer were able to provide the information requested by McGregor. However, it was discovered that he had utilised the information for a purpose different than the one for which it was registered. He was convicted of violating the confidence and privacy of others. [4]

1.3 Cybercrimes other than those mentioned under the it act, 2000

i. Cyber Defamation:

In order to harm someone's company or reputation, cyber defamation is defined as any comment that is maliciously aimed to harm another individual. It is possible to defame someone by using libel or slander. Defamation via computers and the Internet is known as "cyber defamation." For example, someone posts defamatory material about someone on a website or sends defamatory e-mails to all of that person's acquaintances. In addition to the previous list, recently created cybercrimes include bots, botnets, trojans, backdoors, sniffers, SQL injections, buffer overflows, and so on.

ii. Phishing:

It is a type of computer fraud in which a person claims to be a genuine association, such as a bank or an insurance company, in order to steal personal data from a client, such as access codes, passwords, and so on. Examples of legitimate associations include banks and insurance companies. It is normal practise for the party that gathered the personal data to exploit it to their benefit, even if it was obtained by dishonestly claiming the identity of the legal party.

iii. Keystroke Logging:

The action of a user's keystrokes being captured and recorded is included in this. The purpose of this sort of programme is to extract passwords and encryption keys, and in doing so, circumvent any security measures that may be in place.

iv. Data Driven Attack:

A method of attack that is concealed within data that appears to be safe and is then carried out by the software of a user or another entity in order to mount an attack. When it comes to firewalls, a data-driven assault is a cause for worry since it has the potential to breach the firewall in the form of data and then launch an attack on a system that is located behind the firewall.

v. Cyber Stalking:

Despite the lack of a globally agreed-upon definition, cyber stalking is commonly understood as the frequent use of Internet services by the cybercriminal against the victim in order to annoy or threaten them. Stalking, in general terms, refers to repeated acts of harassment targeting the victim, such as following the victim, making harassing phone calls, murdering the victim's pet, vandalizing the victim's property, leaving written messages or items. When a person is stalked, they may do major violent acts, such as harming the victim physically. There are no guarantees; it all relies on how the stalker acts. [5]

2. JURISDICTION AND CYBER CRIME

Unless a court has adequate jurisdiction, its rulings have no legal basis and are of no consequence. It's difficult to enforce Internet Jurisdiction due to the fact that so many people from all over the world are involved in the case. This makes it impossible to determine the exact location of the offender's residence or the event that led to the commission of the crime.... Our IT Act, 2000, passed by the legislature, covers the whole country and includes any violation of the Act performed outside of India by any individual or organisation. As a result, Indian courts now have extraterritorial jurisdiction, allowing them to consider cases involving crimes committed outside of India, regardless of the nationality of the perpetrators. Criminals who commit crimes on behalf of non-resident aliens must do it via an Indian-based computer system or network. [6]

2.1 Evolution of Cyber Laws in India

According to the Indian parliament's decision, it was required to implement General Assembly resolution approved by U.N. Commission of International Trade Law on Model Law on Electronic Commerce (UNCITRAL). Consequently, on 17 May 2000, the Information Technology Act 2000 was approved and put into practise. The preamble of this Act indicates its goal to legalise e-commerce and further reform the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Book Evidence Act1891 and the Reserve Bank of India Act 1934. So that they can effectively govern and oversee cyberworld issues, these Acts have been updated to integrate the modifications made by the Act of 2000. Cybercrimes are addressed in Chapters IX and XI of the Information Technology Act. These are the most essential sections: Ss. 43, 65, 66, 67. Unauthorized access, unauthorised downloading, virus assaults or other contamination that causes damage, disruption, denial of access or interference with the service provided by a person is addressed in Section 43.As a form of punishment, this clause allows for a fine of up to one million rupees. There are penalties of up to three years in jail for "tampering with computer source material," as well as fines of up to two years or both. Sec. 66 of the Penal Code addresses the crime of "hacking with computer system," which is punishable by up to three years in jail, a fine of up to $25,000, or both. Section 67 also deals with the publication of obscene content, which can result in up to 10 years in prison and a fine of up to Rs. 2 lakhs if convicted. [7]

2.2 Impact of Cyber Crime on the Criminal Justice system

The criminal justice system in every region of the world has been significantly altered as a result of the widespread problem of cybercrime. The repercussions are felt much more acutely now, as governments throughout the world work tirelessly to improve the speed and efficiency of the services they offer to their inhabitants by utilising cyberspace and the internet. At some point during the commission of a crime in the modern day, the perpetrator is almost certainly going to employ some kind of electronic device, including a computer or some other type of digital medium. As criminals become more aware of the potential of computers and the internet to facilitate the commission of traditional types of crime, they are beginning to employ these technologies as tools in their own criminal enterprises. Since terrorists and members of organised crime cartels are increasingly using encryption, high-frequency encrypted voice or data links, steganography, etc., a Cyber Crime Investigation Cell is now a necessity for any law enforcement agency that wishes to combat not only cybercrimes but also investigate other traditional or conventional crimes. This is because there has been an increase in the use of these techniques in recent years. The fact that computers and other technological tools have been utilised as instruments to aid the commission of traditional crimes is becoming increasingly clear. The terms "organised crime" and "cyber crime" both refer to types of traditional criminal activity that make use of the internet and other forms of electronic media. [8]

3. CYBER CRIME CHALLENGES

Discussions about the advantages and disadvantages of cybercrime go on and on and on and on... In the battle against cybercrime, we face several difficulties. The following are some of the topics that will be covered:.

- Individual and corporate ignorance about cyber security and a lack of a cyber security culture.
- Inability to execute countermeasures due to a lack of properly educated and certified personnel.
- Specifically for the military, police, and security agency workers, there is a no e-mail policy.
- We've seen cyber assaults not only from terrorists, but also from countries that don't share our values.
- In order to join the police force, you must have a high school diploma or equivalent and have no prior experience working with computers.
- It is impossible for the government to track down the source of these cyber-attacks because of the rapid advancement of cyber technology. [9]

3.1 Way to Reduce Cyber Crime

In order to reduce cyber crime and cyber offence, there are a variety of options available, including the following.

Legal Action: In terms of legal action, the following activities may be useful to minimise cyber crime, and it is essential to take them into consideration:

- Act of 1986 enacted the Electronic Communications Privacy Act
- 1974 federal law on privacy
- A law enacted in 1984 to combat computer fraud and abuse.
- The 1996 Computer Security Act.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Protecting Individuals' Personal Data Act of 2007.
- The Data Integrity and Accountability Act.

4. CLASSIFICATION OF CYBER CRIME

In terms of cybercrime, we may divide it into four main groups, as outlined in the following sections:

I. Crime against individuals

The transmission of Child Pornography, Harassment of any person through the use of a computer such as e-mail, Cyber Defamation, Hacking, Indecent exposure, E-mail spoofing, IRC Crime (Internet Relay Chat), Net Extortion, Malicious code, Trafficking, Distribution, Posting, Phishing, Credit Card Fraud, and Dissemination of obscene material including Software Piracy are examples of the types of crimes that fall It is difficult to imagine a crime that may inflict on an individual more potential damage than this one.

ii. Crime against property

Cybercrimes committed against any and all types of property constitute a separate category of Internet wrongdoing. Computer vandalism, often known as the destruction of the property of another person, as well as threatening behaviour and salami attacks are examples of these types of crimes. This type of criminal activity is typically rampant among financial institutions or for the goal of engaging in criminal activity related to finances. The fact that the change is so inconsequential that it would not typically be noticed is one of the key characteristics of this category of offence.

Iii. Crime against organization

Organizational cybercrime is the subject of the third type of classification for cybercrimes. Cyber Terrorism is a subset of this broader category of crime. Growth of the internet has revealed that Cyberspace's standard is being used to push foreign governments, as well as scare the population of a country. When a human individual "cracks" into a government or military-maintained website, it becomes clear that this is an act of terrorism. Almost everyone in the world believes that any system can be broken.

iv. Crime against society

Cybercrimes against society are the fourth form of cybercrime. There are many other forms of crimes that fall under this umbrella term, including fraud, cyber terrorism, web espionage, and exploitation of children and teenagers via indecent content. Other crimes in this category include cyber contraband, data diversion, salami attacks, and logic bombs. Computers, high-quality scanners, and printers may be used to create fake money notes, revenue stamps, mark sheets, and other documents. By using Web jacking techniques, cybercriminals can get access to and manipulate the content of another person's website in order to further their own ends, whether that be political or financial. [10]

5. CYBER SECURITY

As long as organisations exist, privacy and data security will always be a major priority for them. To put it another way, we're now living in a society where everything is stored digitally or electronically. Social networking sites offer a secure haven for users to communicate with their loved ones. Cybercriminals will continue to target social media platforms like Facebook and Twitter to steal personal information from individuals' homes, as well. When using social networking sites or making financial transfers, be careful to use all the appropriate security precautions.

The above comparison of cyber security incidents reported to Cyber999 in Malaysia from January–June 2012 and 2013 clearly shows the dangers of cyber security. As criminal activity rises, so do the number of security measures in place to combat it. Survey results from Silicon Valley Bank show that corporations feel cyber assaults pose a substantial danger to both their data and their ability to continue operating in the face of a cyber attack.[11]

- More than 98% of companies are increasing or maintaining their cyber security resources, and of those, half are increasing resources devoted to online attacks.
- Major corporations have begun preparing to defend themselves against cyber assaults, not only if they happen.
- Only one-third of respondents are entirely confidence in the protection of personal information, and even fewer are confident in the security measures employed by their business partners.

6. CONCLUSIONS

The constant flux of life is what makes it interesting. Today's perfect and indestructible may not be so tomorrow. Because it's a worldwide phenomena, the Internet is inevitably going to be a magnet for criminal activity. By enacting the Information Technology Act and granting police and other authorities exclusive rights to combat cyber crimes, India has made an important step toward reducing the incidence of this type of crime. Various nations have made similar attempts to combat this threat by implementing national legislation, but it is possible that these efforts will not be as useful as intended in the long term. Still, a worldwide regulation on Internet use is needed to combat the threat of cybercrime and establish a crime-free cyberspace. The best remedy, according to conventional wisdom, is to avoid an accident in the first place. The purpose of cyber laws is to deter criminal activity on the internet by enforcing penalties. However, much work need to be done before cyber rules have a realistic possibility of influencing modern society.

REFERENCES

1. ACM, 1992, ACM Code of Ethics and Professional Conduct, Association of Computing Machinery, USA, October 1992.
2. Saracevic, T. (1996). Relevance reconsidered. Information science: Integration in perspectives. In Proceedings of the Second Conference on Conceptions of Library and Information Science (pp. 201– 218), Copenhagen, Denmark: Royal School of Library and Information Science.
3. Saracevic, T. (1975). Relevance: A review of and a framework for the thinking on the notion in information science. Journal of the American Society of Information Science, 26(6), 321–343.
4. Williams, G.L., Glanville Williams Learning the Law, A.T.H. Smith, Editor. 2006, Sweet & Maxwell.
5. Govil, J., Ramifications of Cyber Crime and Suggestive Preventive Measures, in International Conference on Electro/Information Technology, 2007 IEEE. 2007: Chicago, IL. p. 610-615.
6. Jones, A., Technology: illegal, immoral, or fattening?, in Proceedings of the 32nd annual ACM SIGUCCS fall conference. 2004, ACM: Baltimore, MD, USA. p. 305-309.
7. Majesty, H., Cyber Crime Strategy, S.o.S.f.t.H. Department, Editor. 2010, The Stationery Office Limited: UK. p. 42.
8. ACM, 1992, ACM Code of Ethics and Professional Conduct, Association of Computing Machinery, USA, October 1992.
9. Kubo, Takeaki, 1999, Internet Revolution & Japanese IT Industry, Symposium on Development of Information Industry in the AsiaPacific Region, 5-8 October 1999, Srilanka, page 21-93.
10. Roshan, N., What is cyber Crime. Asian School of Cyber Law, 2008: Access at - http://www.http://www.asclonline.com/index.php?titl e=Rohas_Nagpal,
11. indolink.com (2012). India battles against cyber crime.Retrieved from http://www.indolink.com/displayArticleS.php?id=102112083833.

Corresponding Author

Dr. Monika Mishra*

Assistant Professor, Apex School of Law, Apex University, Jaipur-303002 (Rajasthan)