Asian Journal of Research in Social Sciences and Humanities
ISSN: 2249-7315 Vol. 11, Issue 12, December 2021 SJIF 2021 = 8.037
A peer reviewed journal

AN OVERVIEW OF CYBER-CRIMES AND ITS IMPACT ON ECONOMY

Dr. Ruchi Gupta*

*Assistant Professor,
Himachal Pradesh National Law University,
Ghandal, Shimla, Himachal Pradesh, INDIA
Email: advruchigupta@gmail.com

DOI: 10.5958/2249-7315.2021.00311.7

ABSTRACT

The tremendous growth in the area of communication and digital world led to the potential challenges in the area of cyber law and its implications. Nothing is available without cost and drawbacks. Though it makes the life of people hassle free just on a click of button various things can be done at your ease but it led to other kinds of challenges also. Without technology especially computers everything comes to halt be it business, industries, and government functions and so on. Our economy as well as government various types of businesses are dependent on computers for smooth functioning of their businesses as also the economic progress, so do the criminals are active involving in various kinds of cybercrimes. Therefore, in the current paper a systematic understanding and overview of cybercrimes particularly computer related and their impacts over various areas are discussed.

KEYWORDS: *Cybercrimes, Technology, Business, Consumer, Computer Crime, IT Act* **.**

1. INTRODUCTION

Digital technology and new communication systems have made dramatic changes in our lives. Business transactions are being made with the help of computers. Due to various reasons it is easy to store and access information on computers these days. Thousands of goods and other products and services are delivered and sold online. Online payments, E-billing or E-payments are very common these days. Huge number of people relies on online business for their daily activities and supplies from medicine to luxury. But with the passage of time this system of business is getting worse related with so many issues and challenges leading to financial crisis and economic impact on our economy. This issue requires international cooperation. Some kinds of rules are urgently required which can handle the problem well in time specially when people are working in associations or organizations. So that peace and order can be maintained in the society and whenever someone goes against the law it is termed as disobedience to law or as a crime. **[1]**

Businesses need to take the economic impact of cybercrime more seriously, say researchers, with the cost of cybercrime now up to 0.8% of global gross domestic product (GDP) or $600bn a year, a study has revealed. Europe suffers the highest economic impact of cybercrime, which is estimated at 0.84% of the regional GDP, compared with 0.78% in North America, according to the latest report on the economic impact of cybercrime by security firm McAfee and the Center for Strategic and International Studies (CSIS). “The reality is that cybercrime is just an evolution of traditional crime and has a direct impact on economic growth, jobs, innovation and investment,” he said. “Companies need to understand that in today’s world, cyber risk is business risk.”

In India cybercrimes are increasing at an alarming rate. Internet came in 1994 and IT act 2000 came after six years. With the coming of internet many kinds of crimes associated with internet also came into vogue in different forms and intensity. Example of Jamtara district in state of

Jharkhand is a hub of cybercrimes. Vigorous form of phishing is being conducted from there like credit card frauds and other financial crimes. This resulted in huge financial loss to individuals and in turn to economy. First cyber murder was committed in 2002 in U.S of an underworld don by changing his prescription by hacking the computer in the hospital. So one doesn't need to be physical present to commit these types of cyber attacks on individuals or organizations it can be committed from any jurisdiction into any jurisdiction. **[2]**

Meaning of Cyber Crime:

There are 4 essential elements needed to constitute a crime first is human being, second *mensrea*(an evil intent), third *actus reus* and fourth and last is an injury to another human being or to society at large by such act and when such kind of act is committed in society by depicting such an evil intent through computer or other means of technology is called as cybercrime.

Another definition given by the director of computer crime research Centre during an interview on the 27th April 2004, is that cybercrime is any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them"

1. Cybercrime may also be referred to as computer crime. Crime that uses computer networks to advance other criminal activities. These types of crimes include cyber stalking, phishing and fraud or identity theft.
2. There are acts where computers are used as tool to do unlawful act. This kind of activity involves a change in the way of conventional crimes by using computer. Some examples are:
3. Financial crimes like cheating, credit, card frauds, money laundering etc.
4. Cyber pornography it includes pornographic sites, magazines on computers and the internet to download and photos etc.
5. Sale of illegal articles like weapons, Narcotics etc.
6. Online gambling
7. Intellectual property crimes like infringing trade mark of another, or copyrights etc.
8. Email spoofing: shopping website, asking the recipient to provide sensitive data, such as a password or credit card number by spoofed mails is a common example.
9. Forgery: it is also common these days so many sophisticated forms of computer, software, printers and scanners thereby committing forgery by students in the form of duplicate mark lists or forged docs etc.
10. Cyber defamation: it means defaming someone by circulating or publishing information using a computer or internet like these days social media is very popular to defame anyone.
11. E-Mail Bombing
12. Cyber Stalking**:** a new concern known as: cyber- stalking". Stalking is the crime of following and watching somebody over a long period in a way that is annoying or frightening. Ritu kohli case is one of the cases of cyber stalking where the accused followed her through phone and emails and harassed her so she lodged a complaint and the accused was arrested.

Some Other Types of Cyber Crime: The computer related offences are broadly as follows; -

1. **Dos Attack: -** DoS attack means preventing legitimate users of a service from using that service. It may happen due to:

- Flooding a network; or

- Disrupting connections between the machines; or
- Disrupting service to as specific system or person; or
- Preventing a particular individual from accessing a service; or
- Illegitimate use of resources.

2. **Adware and Spyware:** They are often referred to the programs that get installed on our computer without and with our permission (perhaps permission being granted unwittingly).

The former category is called spyware and the latter adware. These programs can drain computer's resources, slow Internet connection, spy on surfing, and even forcibly redirect Web browser.

3. **Scareware or Fake Anti-virus Programme: -**often an unethical marketing practice is used to create anxiety, or perception of threat to convince an unsuspecting consumer into purchasing and downloading a software of limited or no benefit; it is malware itself. Also known as Scareware or fake anti-virus programme. This is case of fraud or cheating.
4. **Ransomware: -** Ransomware (malware), or extortive malware that holds users' data to ransom.
5. **Hacking, Spam, and Phishing: -** Spam, Spam and Phishing are also common in the Cyber world. They are as follows;

- **Hacking:** cracking system and gaining unauthorized access in to someone's system and information without their knowledge and assent and taking information then misusing it.
- **Spam:** It is an unsolicited e-mail. They are a menace. They should not be sent unless asked for.
- **Phishing:** by this confidential information of the user is accessed to fool them and targets are asked to click on the link that connects to fraud organization's websites or they are asked to provide their confidential information.

Major Challenges in tackling the Cyber Crimes:

Some of the factors which continue to have their impact on the state of cyber security are as follows:

- **Awareness among people is low:** Awareness amongst internal employees is very low. Not many organizations invest in training and improving the cyber security awareness within the firms and enterprises.
- **Inadequate resources:** Very low budget is accorded to cyber security by the enterprises. This is primarily due to the lack of awareness on the impacts of these threats.
- **Poor Identity and Access Management:** There remains a lot of area where the work needs to be done by the enterprises as in this new era at one click of hacker gains entry to the network of enterprises.
- **Ransom ware on the increase:** The recent episodes of malware attacks, viz. WannaCry and Petya, brought home the rising menace of ransomware. The risks of ransomware attack via email, criminals are entering into other vectors. Ransomware attackers have also started to use techniques other than encryption, to deleting or corrupting file headers.
- **Mobile devices and Apps:** Due to unavoidable use of mobile phones by everyone almost in these times it is the best way to use as channel for promoting business so as for

hackers too**.** Financial dealing is activated through mobile apps and the mobile phones are attractive and easy targets in mobile malware.

- **Social Media another menace**: these days almost everyone can be seen on social media platforms which are also an essay option for hackers to gain information and personal details of the users. Many users disclose so many personal details on that which can be easily exploited by the hackers. These days' people easily hack into accounts of the users and demands money from others**.**
- **Prevalence of Obscenity: -** Another area of concern in cybercrimes is obscenity available on internet, lakhs of children specially during pandemic are sitting alone in their houses so one should be careful when one's child is spending alone time with computer. It also contains obscene material. A vulnerable mind can be easily misled by such information.
- **Challenge in preservation and retention of information:** Nothing is confidential in this age of technology. Preservation of information is necessary.

Impact of cybercrimes on various systems

India reported 11.8% rise in cybercrime in 2020; 578 incidents of 'fake news on social media'. The rate of cybercrime (incidents per lakh population) also increased from 3.3% in 2019 to 3.7% in 2020 in the country, according to the National Crime Records Bureau (NCRB) data. The year saw 4,047 cases of online banking fraud, 1,093 OTP frauds and 1,194 credit/debit card frauds, while 2,160 cases related to ATM were reported in 2020.

- **Social Impact**

Having a crimeless society is a myth it is omnipresent and now an inseparable part of our existence. Crime is a social phenomenon and it is one of the features of the all societies, may it be civilized or uncivilized. High crime rate is not because of its nature but due to the disturbances it causes to the society. Some individuals are targets of crime in a more specific sense.

- **Socio-Eco-Political Impact**

The crime is dynamic and changing concept which depends on the socio-economic and political structure of a country. In developing countries, we can see more of economic crimes due to so many factors. Another reason for increase in economic crimes is use of computer technology by the people. Crime is interdependent on above factors. A positive correlation between the population of a nation and increase in economic crimes has been observed. Besides population, the other factors influencing the crime are, rate of urbanization, migration of population from neighboring places, unemployment, income inequality, unaware of computer technology etc. The economic structure of a society also influences the rate of economic crimes. Then the political structure and system also influence the rate of crime in a particular society. So, we can see that everything is interdependent to judge the situation of crime in a society or nation.

- **Cybercrimes and Impact on Industries**

Many big companies are also the victim of cybercrimes but they are not much aware of this fact. a cancer that destroys from within. According the report "Second Annual Cost of Cyber Crime Study – Benchmark Study of U.S. Companies" published by the Ponemon Institute, a study is based on a representative sample of 50 larger-sized organizations in various industry sectors, the impact of cybercrime has serious financial consequences for businesses and government institutions despite the high level of awareness of the cyber threat. The report shows that the median annualized cost of cybercrime for 50 organizations is $5.9 million per year, with a range of $1.5 million to $36.5 million each year per company. The total cost is increased if compared to the first study of the previous year.

- **Impact On Behavior Of Consumers**

The perception of shopping online has changed with the advent of online shopping so is the dark side of cybercrime is attached with e- commerce it has taken various forms. Business houses and corporations need to realize that these kinds of frauds and online businesses have exposed them and the users to more online frauds. So, they should take note of strategic implications to their business future and proper solutions to ensure that these threats are removed or significantly reduced so that internet consumer can repose confidence in the online selling and buying. There is need for the development of models that will allow corporations to study the effects of cybercrime on online consumer confidence and to the benefits attached with the cyber security.

- **Impact over every kind of Business**

According to the FBI and the Department of Justice, cyber-crime is on the rise among American businesses, and it is costing them dearly.

Cyber generated crimes include a wide variety of criminal practices to breach the security of a company technologically. To steal the financial information of the business or its customers is the purpose of the electronic break to install a virus that monitors future online activity of the company or business.

Need for Cyber Law

With the rise in misusing and abusing the technology we need a strict statutory framework to regulate the criminal activities in the computer world. Cyber space is governed by the cyber law. Cyber space includes wide variety of terms like computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, Smart watches and ATM machines etc. cyber law gives legal recognition to digital signatures and electronic records.

Cyber law covers laws relating to:

1. Cyber/virtual Crimes
2. Covers Electronic and Digital Signatures
3. Intellectual Property related crimes
4. Protection of data and Privacy

There are various reasons for conventional law to cope with cyberspace**.**"INFORMATION TECHNOLOGY ACT, 2000" [ITA- 2000] was enacted by Parliament of India to cover and prevent the cybercrimes in the field of e-commerce, e-governance, e-banking as well as prescribes the penalties and punishments in the field of cyber-crimes. The above Act was later amended in the form of IT Amendment Act, 2008 [ITAA-2008]**.** The primary purpose of the information technology Act 2000 is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The IT Act also penalizes various cyber-crimes and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs 1 Crore). **[3]**

2. CONCLUSION:

At the end it can be concluded that the tremendous growth of internet use in world and particularly in India is accompanied by substantial increase in cybercrime and has made India vulnerable to such crimes. These crimes are of global nature and not restricted to boundaries. There is different impact on different kinds of working systems which adds up to build an economy or a strong nation. In today's time everyone is exposed to technology even the kids of three years know how to operate a mobile phone therefore, with every increasing technology we need to have strong and leak proof laws and regulation to curb the menace of cyber-crimes. Efforts of the law-making agencies should be made to keep the crime under control. Therefore, the legislation must be covering each and every aspect of cybercrimes so that a vigilant and constant check can be made over the cybercrimes.

REFERENCES:

1. Das S, Nayak T. Impact of cybercrime: issues and challenges. International Journal of Engineering Sciences & Emerging Technologies, 2013;6(2):142-153.

2. Gupta RK.India: An Overview of Cyber Laws vs. Cyber Crimes: In Indian Perspective, available at https://www.mondaq.com/india/privacy-protection/257328/an-overview-of-cyber-laws-vs-cyber-crimes-in-indian-perspective

3. Introduction to Indian Cyber Law, Fundamentals of Cyber Law document by Asian School of Cyber Laws p.4 available at http://osou.ac.in/eresources/introduction-to-indian-cyber-law.pdf