INTERNATIONAL JOURNAL OF CRIMINAL BEHAVIOR AND SOCIAL POLICIES

VOL: 15 ISSUE: 1
MARCH, 2026
ISSN: 3997-6678

MEASURES AND EMERGING DIFFICULTIES IN INFORMATION TECHNOLOGY ACT

Vartika Pandey
Department of Law, Mangalayatan University, Jabalpur, Madhya Pradesh, India

ABSTRACT

Cybercrime is starting to spread like a parasite in cyberspace. We are indeed dependent on technology nowadays and somehow internet has become a part of our lives. By this rapid development cyber-crime has become a major issue globally. Very few people are convicted of cybercrime; hence actions must be taken to change this. The internet has somehow transcended every aspect of our life. Due of this quick progress, cybercrime has emerged as a significant worldwide problem. Cybercrime is distinct from other kinds of crime that take place in society. The reason is because it has no geographical limits and that no one recognizes who the cybercriminals are as it's difficult to trace them. It has an impact on all relevant stakeholders, including the government, industry, and citizens. With the rising usage of information and communication technologies in India, cybercrime is on the rise (ICT). As according Cyber security Ventures, over the next five years, the cost of cybercrime would increase by 15% annually, reaching $10.5 trillion USD annually by 2025 from $3 trillion USD in 2015. In addition to being exponentially larger than the damage caused by natural disasters in a year, this represents the largest transfer of economic wealth in history and poses a threat to the incentives for innovation and investment. It will also be more lucrative than the global trade in all major illegal drugs put together. In this article, I'll talk about the Measures and Emerging Difficulties in Cyberspace and the significant changes that could eliminate the IT Act's gaps.

KEYWORDS: Cybercrime, Cyber Security, Information and Communication Technologies (ICT), Future Cyber Security, Information Technology Act.

INTRODUCTION

Cyberspace is a domain where data is stored, changed, and exchanged through infrastructure systems connected to networks and systems and the electromagnetic and electronic spectrum. The Internet is a vast, unending area known as cyberspace. You can think of computer transactions as taking place in space, especially when they happen between various computers. Cyberspace is where text and images on the Internet exist. The phrase serves as a moniker for the made-up space in which a virtual object lives when used in connection with virtual reality. A building is considered to be in cyberspace if a computer generates a picture of it that enables the architect to virtually "walk in" and assess the nature of a design. A criminal organizations attack on cyberspace and cyber security is known as cybercrime [1]. Hacking into computers is a type of cybercrime that can be committed through a network system, clicking on strange links, connecting to unsecured Wi-Fi, downloading data and software from dubious sources, wasting energy, emitting electromagnetic radiation, and other methods.

Because it has become a national concern, cyber security is a significant issue that requires urgent attention. Even though the majority of modern electronics, including computers, laptops, and cell phones, come with built-in firewall security software, computers are not always precise and dependable when it comes to safeguarding our data. Due to the government's Internet policy, cyber systems have given rise to the flexibility of illicit usage in today's globe. The economy is at risk from a number of factors, including the Internet, online shopping, selling, and social networking. The Internet has made commercial operations including coding, classification, summarization, and editing simpler. Known as the "global and dynamic domain," it is defined by the simultaneous use of electromagnetic spectrum and cyberspace electronics for the creation, storage, modification, exchange, and extraction of physical resources as well as for usage, removal, information, and disruption [2]. Cyberspace can also be thought of as a hypothetical setting for computer network communication. 1990 The phrase gained popularity in the 1990s during a time of rising Internet, networking, and digital communication use because it was able to include a wide range of novel concepts and advancements in the field.

However, it is through this same cyber network that others intrude upon us and carry out attacks that are harmful to our social, economic, and private lives. Inadvertent side effects include criminal behaviour, spamming, credit card fraud, phishing, and ATM fraud. Interestingly, some academics have asserted that "nobody in the Internet knows a dog [3]". This raises a few legal consequences and concerns. The IT revolution has opened up a lot of doors and opportunities that have a huge impact on the current travel, security, and communications industries. The widespread integration of human activity with electronic infrastructure and resources creates a significant vulnerability that poses a constant risk of misconduct, fraudulent handling, and the failure of computers and computer networks, even though the advantages of the information age are not flawless.

There are advantages and disadvantages to the development of the Internet. The increasing increase in cybercrime in recent years has had a tragically detrimental effect on the nation's social economy. Unhappiness with cyber and personal security has resulted from immoral cyberspace users' ongoing use of the Internet to conduct crimes during the past twenty years. The trend has just lately gotten worse, thus that there is an urgent need for legislation that safeguards users of the internet and the online environment.

Future of Cyber Security and Impact of Cyber-Crimes in the World Economy

There is a substantial threat that information technology will damage or interfere with the services that are essential to our economy and the daily lives of billions of people as it continues to permeate physical infrastructure operations. The safety and adaptability of cyberspace are now security objectives due to the dangers and potential consequences of cyber security. Cyberspace is the term for the Internet's boundless expanse. It alludes to a network of interconnected information technology components, which is where many of today's communication technologies are found. In the next five years, the cost of cybercrime is predicted to rise sharply, from $8.44 trillion in 2022 to $23.84 trillion in 2027, according to predictions from Statista's Cyber security Outlook. According to Cyber Crime Magazine, cybercrime includes "data damage and destruction, theft of money, lost productivity, and theft of intellectual property, theft of personal and financial data, embezzlement, fraud, and post- attack

disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm." The industry of cybercrime is flourishing. Both the returns and the risks are favorable. We predict that cybercrime will likely cost the global economy more than $400 billion annually. Losses of $375 billion would be a reasonable estimate, while $575 billion may be the highest [4]. Governments and businesses significantly underestimate the risk that cybercrime poses to them and how fast that risk might increase. Even the smallest of these estimates is greater than the national revenue of the majority of countries.

According to Cyber security Ventures, during the next five years, the cost of cybercrime would increase by 15% yearly, reaching $10.5 trillion USD annually by 2025 from $3 trillion USD in 2015. In addition to being exponentially larger than the damage caused by natural disasters in a year, this represents the largest transfer of economic wealth in history and poses a threat to the incentives for innovation and investment. It will also be more lucrative than the global trade in all major illegal drugs put together. The headline attempts to place a price on cybercrime and cyber-espionage, but the dollar amount raises crucial concerns regarding the harm done to the victims as a result of the cumulative impact of losses in cyberspace. Hundreds of millions of people have had their personal information taken as a result of cybercrime, with incidences affecting more than 40 million people in the US, 54 million in Turkey, 20 million in Korea, 16 million in Germany, 20 million in China and more than 600 thousand in India in the past year [5].

According to one prediction, there will be more than 800 million unique recordings in 2013 [6]. The price of this alone might reach $160 billion annually. Cybercrime has negative effects on employment that are significant for industrialized nations. Cybercrime has the impact of shifting employment away from positions that add the most value. Employment can be impacted by GDP changes of any size. Studies on the relationship between employment and export growth indicate that the losses from cybercrime could cost as many as 200,000 American jobs, or about a third of 1% less employment for the US, in the US alone [7]. According to data from the European Union, 16.7 persons were employed for every million Euros in exports to other countries. After adjusting for national disparities in IP-intensive jobs, Europe might lose as many as 150,000 jobs as a result of cybercrime, or 0.6% of the overall unemployed [8].

According to Lt Gen (Dr.) Rajesh Pant, national cyber security coordinator, cybercrimes cost India 1.25 lakh crore in losses in 2019, and dangers will only grow as the nation begins to build smart cities and roll out 5G networks, among other efforts. He claimed that there was a significant gap in the market for Cyber security solutions and that there were just a few Indian companies producing them. He also advocated for the creation of an industry conference specifically for Cyber security to create reliable homegrown defenses against cyber-attacks [9]. A global system of interconnected computer network is built using the electrical medium of cyberspace to enable online communication.

The TCP/IP protocol is used by a sizable computer network, which is made up of numerous other computer networks throughout the world. These days, crimes are committed online. These include crimes that have both financial and human repercussions, such as the production and distribution of child pornography and child abuse conspiracies, financial and banking fraud, intellectual property infringement, and

other offences. A vast array of interconnected and crucial networks, systems, services, and resources, collectively known as cyberspace, are essential to the financial awareness and national security of the world's countries. The way we communicate, travel, power our homes, manage our economy, and access government services has all changed because to the internet. The foundation of technology, procedures, and methods used to safeguard data against attacks, deterioration, or unauthorized access to networks, computers, programmes, and data is known as cyber-security. Cyber-security is the term used to describe security in computer or cyber contexts. To maintain Cyber security, both citizens and their information systems must work together. Our cyber-security flaws are posing a threat that is growing quicker than we can handle. Due of the violation's infringement and increased allowance for other issues, it is impossible to concentrate effort on just one part of the infraction. We can therefore infer that we will have to deal with cyber security breaches on an ongoing basis.

To safeguard the digital platform as well as the assets of businesses and consumers, cyber security is a combination of tools, policies, security ideas, security officers, rules, risk management strategies, activities, training, best practices, guarantees, and technologies. A group of coordinated crimes known as "cybercrime" target both cyberspace and Cyber security. Cybercrime is defined as criminal action carried out online and on computers. These include sending computer data, unauthorized access, and computer access to or through a computer system. Theft of billions of dollars from internet bank accounts is included, as is downloading illicit music files. Cybercrime also encompasses non-financial offences like developing and disseminating viruses on other computers or publishing private company data online. Identity theft, in which criminals exploit the Internet to steal other users' personal information, is arguably the most striking aspect of cybercrime.

Identifying Cybercriminals

The Age Groups of Cybercriminals are Extremely Diverse

Youngsters (age group 9-16): It may be difficult to believe, but children can also engage in cybercrime, whether consciously or unknowingly. Teenagers make up the majority of inexperienced hackers. Being able to hack into a computer system or a website seems to be a source of pride for these kids. They could also carry out the offences without being aware that they are doing something wrong [10].

Syndicated hackers or Hacktivists: Hacktivists are a group of hackers that collaborate for a specific goal. Most of these organisations have political motivations. In contrast, in other situations, their motivations may be anything from social activism to religious activism [11].

Unfulfilled Employees: It is difficult to imagine how bitter disgruntled employees might turn. Up until today, these disgruntled workers could go on strike against their employers. Disgruntled employees can now cause a lot more harm to their companies by committing crimes using computers, which can bring their entire system to a halt, thanks to the growing reliance on computers and the automation of procedures.

Professional Hackers: Information is now stored in electronic form in commercial organisations as a result of extensive computerization. Rival organisations hire hackers to steal additional commercial secrets and information that could be useful to them. It is seen redundant to require physical presence to gain access if hacking can retrieve the relevant information from competitors' businesses. This increases the

incentive for businesses to employ skilled hackers to perform their dirty work [12].

Information Technology Amendment Act Issues and Challenges

While the Act has been successful in laying out the framework of legislation in Cyber Space and addressing a few urgent issues about technological misuse, it has a few significant flaws that have not been addressed. Many experts contend that the Act is toothless legislation that hasn't been totally successful in imposing punishments or sanctions against offenders who chose to abuse the reach of online, including Supreme Court lawyer and activist for cyber rights Pawan Duggal. There are some topics of cyber law that require attention as given below:

Phishing

Phishing is the criminally fraudulent technique of trying to get private data, such as usernames, passwords, and credit card numbers, by posing as a reliable source via electronic communication. Phishing frequently uses email to trick people into entering their personal and financial information on a website. One method of social engineering used to deceive consumers is phishing. The Indian Penal Code refers to cheating, but that is not enough to stop phishing activity. There is no regulation against phishing in the Information Technology Act. A clone of the SBI website was recently utilized in a phishing assault on State Bank of India clients. Even SBI has not informed its consumers, which is worse. Legislation that forbids the practice of phishing in India is thus urgently needed.

Spamming

Unsolicited bulk email is one way to define spam [13]. It was at first thought of as merely an annoyance, but now it is causing serious economic issues. To address the spam issue in the absence of appropriate technical protection, strict legislation is necessary. The topic of spamming is not at all covered under the Information Technology Act. Anti-spam laws have been passed in the USA and the EU. In fact, spammers who violate Australia's strict spam rules might face daily fines of up to 1.1 million dollars [14].

Data Security for Online Banking

Data protection regulations are primarily intended to protect the rights of the person whose personal information is handled and processed by others. Numerous third parties are also involved in Internet banking, in addition to banks and their clients. Information that banks hold about their clients, their transactions, etc., frequently changes hands. The banks are unable to save information on their own computer networks. Preventing data leaks or tampering involves high risks, necessitating sufficient legal and technical protection. India does not even have a legislation controlling a specific subject like the safety of data in electronic banking. Although the Information Technology Act mentions unlawful access, it makes no mention of preserving the integrity of consumer transactions. The statute does not impose any obligations on banks to safeguard client and customer information. In accordance with a data protection law that was passed in the United Kingdom ten years ago, in 1998, banks or anybody else who has sensitive information may be held accountable for damages if they fail to maintain effective security protection for such data. Due to the lack of a relevant statute in India, a bank's obligation would be determined by the terms of the contract.

Privacy Protection

As information technology becomes more essential in the personal, professional, and economic arenas, privacy and data protection are significant challenges that must be addressed. When personal data or information is transmitted outside of their respective jurisdictions, [15] the European Union and the United States have strong policies relating to privacy and protection. It is also important to point out that India has lost out on significant foreign investment and other commercial prospects as a result of the lack of a dedicated privacy law. This shortcoming has also prevented the actual expansion of electronic commerce.

Identity Theft

Identity theft is a developing issue on a global scale. The IT Act of 2000 does not address this problem. This is a significant disadvantage given that the majority of the outsourcing work that India performs calls for Indian businesses to guarantee there is no identity theft. In fact, one of the main causes of a significant uproar over an event involving personal data of UK clients and an Indian web marketing company was identity theft.

Cyber Warfare or War on the Internet

The Act also doesn't address the problem of cyber war. Any legal system must make provisions in accordance with the international legal order, which is an essential component [16]. China has launched numerous cyber-attacks against India in recent years, and Chinese hackers have successfully bypassed the Firewalls on Indian databases like a Mongol army on the rampage. Several confidential documents were given to the perpetrators of the 26/11 attacks from nearby countries who were plotting against India as intelligence. The Act does not contain any provisions that would hold these offenders accountable for their deeds. There is a need for overhauling the Cyber security legal regime in the country, The IT (Amendment) Act, 2008, which rendered practically all cyber offences, with the exception of a few, bailable charges, was a historical error. The number of convictions for cybercrime in the nation is in the low single digits since the emphasis is primarily on increasing the scope of civil liability and decreasing the scope of punishment.

The most common kind of modern cyber "misuse" is the downloading of movies using peer-to-peer networks. This is a widespread breach of copyright rules, but there are so many offenders that it is impossible to stop it with an effective remedy [17]. Website access is frequently blocked by the government as a means of reducing the growing threat of cybercrime. According to Article 19(1) (a), this is believed to be a severe action that violates the freedom of speech and expression. The Madras High Court has issued an injunction prohibiting users from accessing torrent websites to discourage them from downloading copies of the Tamil film "Three" from the internet [18]. Blocking access to the entire website is an overly strict policy, even though it would be fair for only the one movie. As is true in the case of the government, it has been claimed that ignorance can be a hazardous thing. It attempts to put precautions into place based on its scant understanding. Users are becoming more skilled and knowledgeable every day, and they are able to get around security measures while legislation is still trapped in the prehistoric era of the internet.

On the internet, there are copyright and trademark infringements, yet neither the Trade Mark Act of 1994 nor the Copyright Act of 1976 directly addresses these issues. Therefore, there is no enforcement infrastructure to guarantee the security of

domain names on the internet. The Negotiable Instruments Act of 1881 does not provide protection for the transmission of electronic cash or online transactions. Only Sections 43 (penalty for damage to computer or computer system) and 72 (Breach of confidentiality or privacy) make reference to online privacy protection; these sections, however, do not prevent violations from occurring in cyberspace.

The Information Technology Act of 2000 exempts from liability even Internet Service Providers (ISPs) who send some third-party information without human participation. If one can demonstrate that the offence was committed without his knowledge or that he took reasonable steps to stop it, one can readily seek refuge under the exemption clause.

Because the terms "due diligence" and "lack of information" are not defined anywhere in the Act, it is difficult to demonstrate that the infraction was committed. Sadly, the Act makes no mention of how extraterritoriality will be used. The Act, which was created to investigate into cybercrime and which on the surface appears to be a worldwide issue without territorial limits, utterly ignores this aspect [19].

Suggestions for Strengthening the it Act

The severity of punishment for the bulk of cyber offences was lowered under the IT (Amendment) Act, 2008 there needs to be a remedy for this.

The majority of cybercrimes should not be subject to bail.

The bulk of crimes committed using mobile devices are not covered by the IT Act. There needs to be a solution for this.

In order to increase the law's effectiveness, a thorough data protection system must be included.

A complex legal framework is required to preserve both persons' and institutions' privacy.

The IT Act needs to include cyber war as an offence.

Parts of Section 66A of the IT Act go beyond what the Indian Constitution deems to be legitimate limitations on the right to free speech and expression. To make the provisions enforceable under the law, these must be eliminated.

CONCLUSION

If the situation remained unchanged, we might conclude that cybercrime is merely another problem in society that diverts at most 8% of worldwide income from legal to illicit activity. This image not true. First, as more company operations go online, as more people connect to the Internet globally, as more autonomously devices are connected (the "Internet of things"), the potential for cybercrime will proliferate. The industry of cybercrime is still expanding. The ability of acquiring nations to use IP to develop competitive goods will also improve, which will lead to an increase in the losses caused by IP theft. Therefore, businesses that don't sufficiently defend their networks will experience a growing competitive disadvantage. As cybercrime slows down global innovation by lowering the rate of return for investors and innovators, there are costs to nations in terms of jobs and trade balances as well as a worldwide cost. Those nations who are unable to fortify their cyber defenses will be at a disadvantage. Losses from cybercrime will increase over time, if no other adjustments are made.

The inadequacies of the Indian IT Act legislation and the ensuing realistically anticipated issues serve as further evidence that criminal law cannot be liberally interpreted, particularly with regard to internet regulations. Given that cyberspace allows for certain freedoms of action that make it easier to break the law, any regulatory

mechanism or legislative measure must aim to be as precise as possible. Although the situation is not hopeless, it is important to consider what can alter this scenario. The loss from cybercrime could be decreased with better technology and stronger protection. The cost of cybercrime may be decreased by agreement on and use of Cyber security standards and best practices. Losses may be decreased by international cooperation on law enforcement and state behaviour that included constraints on crime, especially if this cooperation included agreement to uphold already-made international obligations (such the WTO's agreements to safeguard intellectual property). Governments must do a better job of accounting for loss, and businesses must do a better job of assessing risk, if we are to make headway on these improvements.

Without these adjustments, we believe there are two conceivable results. In the first, the cost of crime for industrialized nations would essentially remain unchanged, at least in terms of a share of GDP, but the overall cost would rise as new players and emerging nations accelerated their use of the Internet. The cost to wealthy economies would rise in the second scenario as more activities moved online and hackers became better at making money off of what they could take. Losses from cybercrime do not appear to be decreasing in any plausible way. The world is expected to see more losses and slower development.

REFERENCES

Bidgoli Hussein. The Internet Encyclopedia, John Wiley & Sons Publication, New Jersey; c2004. 1.

Divya Bhati. India Today: Personal data of 6 lakh Indian hacked and sold on Bot markets for Rs 490 each: study reveal Available at: https://www.indiatoday.in/technology/news/story/personal-data-of-6-lakh-indian-hacked-and-sold-on-bot-markets-for-rs-490-each-study-reveals-2307151-2022-12-09 (Visited on 12 January 2023).

Ghosh S, Turrini E. Cybercrimes: A Multidisciplinary Analysis, Springer-Verlag Heidelberg Publication, Berlin; c2010. ISBN: 978-3-642-13547-7.

Gurjeet Singh, Jatinder Singh. Investigation Tools for Cybercrime, International Journal of Computer, ISSN: 0974-2247. 2013;4(3):141-154.

Halder D, Jaishankar K. Cyber-crime and the Victimization of Women: Laws, Rights, and Regulations, Hershey, PA, USA: IGI Global; c2011. ISBN: 978-1- 60960-830-9.

Halder D, Jaishankar K. Cyber-crime and the Victimization of Women: Laws, Rights, and Regulations, Hershey, PA, USA: IGI Global; c2011. ISBN: 978-1- 60960-830-9.

International Trade Administration 2012, Jobs Supported by Exports: An Update, Available at: http://www.trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/ tg_ian_003639.pdf (Visited on 12 January 2023).

John Hawes 2014. 2013 An Epic Year for Data Breaches with over 800 Million Records Lost, Naked Security, Available at: http://nakedsecurity.sophos.com/2014/02/19/2013-an- epic-year-for-data-breaches-withover-800-million- records-lost/ (Visited on 12 January 2023).

Klaviyo. Understanding Australia's anti-spam legislation; c2022. Available at: https://help.klaviyo.com/hc/en- us/articles/4406840113563-Understanding-

Australia-s- anti-spam-legislation (Visited on 12 January 2023).

Moses AA, Hight CI., Cybercrime detection and control using the cyber under identification model, International Journal of Computer Science and Information Technology and Security, ISSN: 2249-9555. 2015;5(5):354-368 Computer Misuse Act, UK. Available at: http://www.opsi.gov.uk/acts/acts1990/UKpga 19900018 en_1.htm (Visited on 12 January 2023).

N Sousa, JM Rueda-Cantuche, I Arto, V Andreoni. Extra: EU Exports and Employment, Chief Economists Note, European Commission, Trade; c2012. Available at: http://trade.ec.europa.eu/doclib/docs/2012/may/tradoc 14 9511.%202_24.05.2012.pdf. See also: Unemployment Statistics, European Commission: Euro Stat, http://epp.eurostat.ec.europa.eu/statistics explained/index.php/Unemployment_statistics; epp.eurostat.ec.europa.eu/cache/.../3-31012014-AP- EN.PDF (Visited on 12 January 2023).

Sruthijith KK, Harsimran Julka. File-sharing sites like Vimeo.com, Torrentz.eu & others blockage sets off torrent of abuse; c2012. Available at: https://economictimes.indiatimes.com/tech/internet/file-sharing-sites-like-vimeo-com-torrentz-eu-others-blockage-sets-off-torrent-of-abuse/articleshow/13231127.cms?from=mdr

Steve Morgan, Forbes: Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Available at: https://www.forbes.com/sites/stevemorgan/2016/01/17/cy ber-crime-costs-projected-to-reach-2-trillion-by- 2019/?sh=1ea418593a91 (Visited on 12 January 2023).

Sunil C Pawar, Dr. RS Mente, Bapu D Chendage. Cybercrime, cyber space and effects of cybercrime, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307. 2021 January-February; 7(1)210-214. (Visited on 12 January 2023). Available at DOI: https://doi.org/10.32628/CSEIT217139. Journal URL: https://ijsrcseit.com/CSEIT217139.

Sunil Pawar C, Dr. Mente RS, Bapu Chendage D. Cyber Crime, Cyber Space and Effects of Cyber Crime, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307. 2014;7(1):210-214. Available at: https://doi.org/10.32628/CSEIT217139 Journal URL: https://ijsrcseit.com/CSEIT217139 (Visited on 11 January 2023).

Techtarget. Hacktivists; c2022. Available at: https://www.techtarget.com/whatis/definitions/Cyber (Visited on 12 January 2023).

The Hindu. Cybercrimes caused loss of ₹1.25 lakh crore; c2020. Available at: https://www.thehindu.com/business/Economy/cybercrim es-caused-loss-of-125-lakh-cr/article32903568.ece (Visited on 12 January 2023).

Webroot. The Dangers of hacking and what a hacker can do to your computer; c2020. Available at: https://www.webroot.com/in/en/resources/tips-articles/computer-security-threats-hackers (Visited on 12 January 2023).