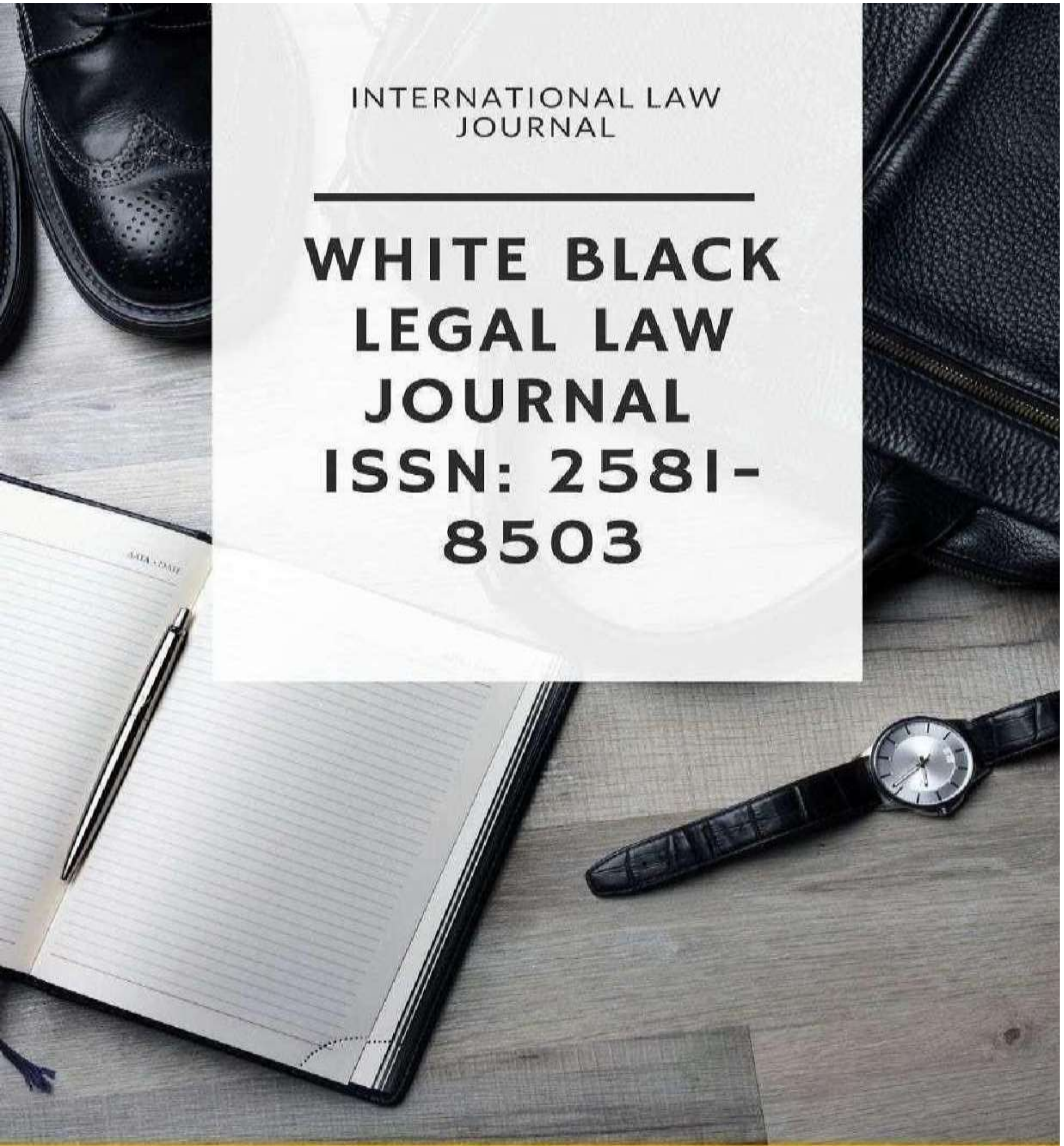

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

"CYBER CRIME AND JURISPRUDENCE: INDIAN AND GLOBAL PERSPECTIVES"

AUTHORED BY - ABHISHEK KUMAR[1]

> ***"Cybersecurity is much more than an IT topic; it's a boardroom topic and a national security issue."***
>
> *— Klaus Schwab*[2]

ABSTRACT

The digital era has precipitated a significant transformation in the methods of criminal commission and their management. Cyberspace has emerged as a new battleground, characterized by the prevalence of offenses such as hacking, identity theft, cyberstalking, and online fraud. This research paper analyzes the influence of cyber laws on information security, emphasizing a comparative study between India and the United States. The paper initiates by delineating the progression of cybercrimes and examines their categorization, characteristics, and the distinct issues they provide. This analysis examines India's Information Technology Act of 2000 and its relationship with established legislation, including the Indian Penal Code and the Evidence Act. Conversely, the paper examines significant U.S. legislation, including the Computer Fraud and Abuse Act and other federal acts pertaining to cyber offenses and digital data protection. This article examines pertinent legal statutes, significant case law, and governmental initiatives to elucidate how various nations have addressed the increasing menace of cybercrime. Although India has enacted laws to enhance cyber security, significant deficiencies persist in enforcement, awareness, and cooperation. The United States, with a more advanced cyber legal framework, provides valuable insights, particularly on jurisdiction, law enforcement, and court response. The comparison indicates that while both nations are diligently striving to safeguard information in the digital realm, India need further enhancement of its legal and institutional structure. The report finishes by presenting pragmatic recommendations for reform, such as improved cyber policing, public education initiatives, law enforcement training, and more international collaboration. Only via such extensive initiatives can governments aspire to address the rising issues of cybercrime and protect their digital landscapes.

[1] LL.M Student At Mulana Azad National Urdu University, Hyderabad

[2] James Comey, *Interview by Scott Pelley*, 60 Minutes, CBS News (Oct. 5, 2014), available at https://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-cybercrime-60-minutes/.

INTRODUCTION

Crime waves are increasingly recorded in hours and minutes, rather than months and years. The world is being recreated in the form of a global village by the new electronic interdependence. [3]If you are familiar with both your adversary and yourself, you need not be concerned about the outcomes of a hundred battles. If you only know yourself and not your adversary, you will lose every victory you achieve. Assuming you know neither yourself nor the foe, you will surrender in each fight."

Crime has existed and will continue to exist since the dawn of society. As long as society continues to strengthen its security measures, criminals will adapt their tactics.[4]Since man's fall, crime and criminality have been associated with him. In the face of development, crime continues to try to conceal itself and remains elusive. Because the bond between family and community was much stronger than that of the individual, the injured party and his kindred could avenge the wrong through private vengeance and self-redress, and recourse to legal remedy was considered only an optional alternative to self-redress, English society prior to the 10th century confused crimes with torts. Depending on the type and scope of the crime, several countries have used various strategies.

The nature of the harm and the victim's social standing were factors in determining the amount of recompense that was anticipated from the wrongdoer at the time. We can claim that, in contrast to now, social connections were not governed by the law in ancient times. In the 12th and 13th centuries, early English culture only regarded some actions as crimes if they were committed against the state or a particular church. Early societies solely adhered to the law of wrongs because there was no distinction drawn between the law of crimes and the law of torts. In modern legal systems, the law is applied immediately after an offense is committed, regardless of the victim's wishes; however, in earlier societies, the law was only applied when both parties wanted to submit to the judgment. It was once thought that no one, not even law enforcement, was involved in a crime during the 18th century, which is also known as an era of miraculous reorientation in criminology. Only the offender could confess criminal culpability for the crime. Evidently, at that time, the concept of wrongdoing was tied to the social structure in place.

[3] Marshall Herbert MeLuhan, *"The Promise of Global Networks",*, Annual Review of Institute for Information Studies, 6 (1999).
[4] https://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en.

The terms "PC crime," "cybercrime," "e-crime," "howdy tech crime," and "electronic crime" generally refer to crimes in which a PC or organisation serves as the source, device, target, or location of the crime as well as to more common crimes involving computers, such as juvenile erotica and Web misrepresentation.. In addition to cybercrime, there is also "PC supported crime," which refers to the use of computers for record-keeping and communication by criminals. There are "no cyber-borders between nations" and cybercrime is "global" or "transnational."[5]

In order to safeguard their citizens and organisations against cyber attacks, India and the USA have adopted a number of laws and regulations. In this analysis, we'll look at how cyber laws in India and the USA affect information security.

India has a number of laws that address information security and cybercrime. The primary law governing cybercrime in India is the Information Technology (IT) Act, which was passed in 2000. Digital signatures and electronic documents are given legal legitimacy, and it defines different cyber offences and their associated consequences. A Cyber Appellate Tribunal is also created by the legislation to deal with legal issues arising from cybercrime.

Various federal and state laws address cybercrime and information security in the USA. The main federal statute that addresses crimes involving computers is the Computer Fraud and Abuse Act (CFAA). The law makes hacking, unauthorised access to computer systems, and other online crimes illegal. Information security is also covered by a number of other laws, including the Health Insurance Portability and Accountability Act (HIPAA) and the Cybersecurity Information Sharing Act (CISA).

Historical Development of Cyber Crimes:

Each field of study and mastery fosters a typical collection of information that recognizes proficiency from novices. One part of the corpus of knowledge is a common history of major occasions that have influenced the growth of the discipline.

"Learning the names and notable occurrences associated with their field aids newcomers in understanding references from more experienced professionals and helps them contextualise

[5] D. Latha, Jurisdiction Issues in Cybercrimes, Law Weekly Journal, vol.4,(85), 2008,available at www.scconline.com,.

new events and patterns. Investigating a phenomenon's historical background comes first in any analysis.

The main driver of cybercrime, an evil, is the increasing reliance on computers in modern society. Numerous crimes can be committed with correspondence technology.[6] Generally, digital violations can be classified into different structures including right off the bat, carrying out new offenses by utilizing new advances like digital wrongdoings against PC frameworks and information and furthermore, carrying out old offenses by utilizing new innovations like utilizing PC networks for working with the commission of digital wrongdoing."

As early as the 1990s, it was claimed that the Internet was a special medium with the quickest pace of diffusion in human history. "Today, there are not many individuals whose lives are not impacted valuably and additionally hurtfully by the innovation of the Web time. Positively, the ability to quickly share and distribute knowledge has brought about unheard-of improvements in commerce, entertainment, social contact, and education. On the down side, it's made it more likely that crimes will be committed. Criminals can now commit large-scale crimes for practically no money and with considerably lower odds of getting caught because to information technology. Online criminals typically do not have to worry about encountering law enforcement or witnesses, in contrast to those who commit classic economic-motivated crimes like burglaries, robberies, and bank heists. In the last ten years, technology has changed how teenagers interact with one another and communicate with one another. The growing reliance of children on innovation is well documented.[7]

Evolution of Computer:

A computer is a programmable device designed to successfully and automatically carry out a collection of mathematical operations or intelligent tasks. There have been many significant events in the history of computers. "Since the introduction of computers and computer regulation are inextricably linked, determining when they began is difficult. The world was introduced to the ABCs of computer building by Blaise Pascal, who built the first sophisticated

[6] *Beza's initiative for safe and secure computing in Botswana*, https://www.bezaspeaks.com/cybercrime/history.htm.

[7] Kathy Martinez Prather and Donna M. Vandiver, "Sexting among Teenagers in the United States: A Retrospective analysis of Identifying Motivating Factors, Potential Targets and the Role of a capable Guardian", International Journal of Cyber Criminology, (2014) available at: http://www.cybercrimejournal.com/pratherVandiverijcc2014vol8issue1.pdf (visited on March 9, 2017).

but non-electronic computer in 1642. [8] The first mechanical computer, which was created by Charles Babbage, eventually gave rise to even more astounding concepts. He started afresh in 1822 by developing the contrast motor, which is intended to assist the brain in understanding the advantages of polynomial powers. In terms of digital crimes, it is possible to trace the evolution of computers back to 1896, when Herman Hollerith created the first punch card arrangement machines for the Assembled Provinces of America (USA) evaluation department to use in organising and analysing data. Whatever the case, IBM acquired it in 1924. Following this, in 1946, Drs. J. Presper Eckert and John Mauchly developed the Electronic Mathematical Integrator and Computer (ENIAC), which was the first advanced computer. From there, they developed the Universal Automatic Computer (UNIVAC), which was the first computer that was actively supported by money.

History of Cyber Crimes:

One could say that the history of cybercrime is brief yet incredibly interesting. Regarding the veracity of the existence of this new assortment of misbehaviour overall, there are diverse points of view. Some claim that since people were involved in using machines for improper reasons when the computer was developed alongside the first math equipment, cybercrime has existed for as long as computers have. "In actuality, the history of digital wrongdoings started with the programmers who, right off the bat, tried to break into computer networks simply for the adventure of getting to unquestionable level security organisations or to acquire sensitive or got data or any confidential for individual advantages or for retaliation. The brief authentic improvement of cybercrime in the utilization of computers and computer networks is examined as under:”

Early History:

Determining the exact time the initial computer-related violation took place is undoubtedly difficult. because social data occurrences and a mechanical cryptographic system may be traced back more than 5,000 years.[9] “Often, early computer violations involved the disruption of the significant distance between phone organizations and the physical harm to computer frameworks. The ability to encrypt and decrypt data was available in 1900 B.C., and an

[8] Wayne Williams, *The evolution of the computer -- from 1613 to 2013*, (Sept. 5, 2014), https://betanews.com/2014/09/05/the-evolution-of-the-computer-from-1613-to-2013/.

[9] Frederick B. Cohen, Protection and Security on the Information Superhighway, (1995)

Egyptian employed it. Following this, Julius Caesar instituted standard letters in proper order in official correspondences between the years 100 and 44 B.C. for the purpose of maintaining data security. The early history of digital wrongdoings dating back to the 1820s has been researched. The short early history of digital wrongdoing in the utilization of computers and computer networks is examined as under:"

Modern History:

"Today, lawbreakers that enjoy cybercrimes are not driven by inner self or mastery. All things considered, they need to utilize their insight to rapidly acquire benefits. They are utilizing their skill to take, beguile and take advantage of individuals as they find it simple to bring in cash without taking care of a legit day's responsibilities. Current cybercrimes are very unique from old-school crimes. These crimes don't need actual presence of the criminals. The short current history of cybercrimes in the utilization of PCs and PC networks is examined as under:"

In the period of 2000 to 2003 — Reputation and Individual Test:

The Information Technology Act (ITA), 2000 was passed by the Indian Parliament with the intention of combating cybercrimes and providing an official framework for online business dealings. This was the very first cyberlaw in India that specifically addresses cybercrimes. It handles a variety of offences committed in an electronic setting or involving computers, computer systems, or computer networks. Oddly, neither this definition nor the word "cyber wrongdoing" or "cyber offence" are used under the Information Technology Act of 2000. Numerous provisions of our present laws, such as the Indian Penal Code of 1860, the Indian Evidence Act of 1872, the Bankers Book Evidence Act of 1891, and the Reserve Bank of India Act of 1934, are altered by this Act.

"In ***Rediff Correspondences Ltd. V. Cyberbooth*** [10]case, The Yahoo judgement was emphasised once more. To combat the cybercrimes in this condition, numerous issues are needed. The fundamental problem is that India lacks a comprehensive legal and administrative framework for policing a variety of cybercrimes, including hacking into secured systems and distributing false Computerised Mark Testaments in tourist hotspots or for fraudulent purposes. Additionally, the Indian Penal Code, 1860 has been modified by the IT Act 2000; nonetheless, the alterations have been made so that the scope of archives indicated in several lawbreaker

[10] AIR 2000 Bom 27.

arrangements can now include electronic records. Then there are other cybercrimes like cyber stalking, cyber harassment, cyber disruption, and so forth that are also not at all covered by the Indian Penal Code. In this case, the aggrieved party also filed a lawsuit seeking an extremely long-lasting injunction prohibiting the defendants from using the domain name "RADIFF" or any other misleading term similar to the offended party's mark or name "REDIFF." In this case, the Court approved a restraining order against the defendants and also excused the Unique Leave application submitted by Cyberstall to the Supreme Court.

From the Period of 2011 to work date:

“In India in the radiance of a progression of captures made under section 66A of the Information Technology Act, 2000, ***Shreya Singhal v. Union of India***[11] is the situation where the writ the request was recorded in broad daylight interest under Article 32 of the Constitution of India for looking to strike down Section 66A as unconstitutional by contending that part 66A is so wide, unclear, and unequipped for being decided on true standards that it is defenseless to wanton maltreatment. It was also argued that neither the General Conditions Act nor the Information Technology Act define the phrases "offensive," "threatening," "irritation," "risk," "block," or "affront." Referring to the arrests made under Section 66A, the attorney argues that the expansive legislative language of the Part seriously discourages residents from exercising their constitutionally protected right to free speech because of their paranoid fear of being found guilty of petty offences (the "chilling impact"), which violates their constitutional right to freedom of expression and expression of their thoughts and ideas under Article 19(1)(a). Furthermore, Section 66A violates Articles 14 (Right to Equality) and 21 of the Constitution regardless of whether it passes the "sensibility" test outlined in Article 19(2).

“The Hon'ble Supreme Court pronounced segment 66A as unconstitutional completely and against the ability to speak freely and articulation and struck it down in ***Shreya Singhal & ors.v. Union of India.*** Police in several jurisdictions have taken use of this clause to detain innocent people for publishing straightforward comments about community and policy-driven issues on systems administration forums. This section led to the arrest of a huge number of people for posting what was allegedly frightening content online.

[11] AIR 2015 SC 1523.

Meaning Concept & Classification of Cybercrimes:

From the very outset of the new thousand years, person to person communication locales have become very well known. These destinations have given a space to numerous to vent their sentiments, get new and interface with old friends.146 However these destinations have been abused by cybercriminal bunches sadly for satisfying their illegal purposes. Next to each other individuals have begun to invest increasingly more energy on such organizations throughout the course of recent years in light of the fact that the people groups progressively depend on them. In the cutting edge time span the advancement of Information Technology impacts the existence of individuals from one side of the planet to the other. New developments and disclosures step by step has extended the logical degree along with bringing new difficulties for legal world. The rapid advancement of this technology has prompted the conduct of new types of crimes in cyberspace today and will likely lead to increased global concern in the future.

Concept of CyberSpace:

William Gibson coined the phrase "cyber space," which he subsequently described as "a suggestive and essentially insignificants trendy expression that could act as a code (changing a text to cover its significance)" for his cybernetic thoughts in general. Today, it is used to portray anything having to do with computers, information technology, the internet, and various web cultures.[12] 'Cyber Space' is a term that is frequently used to refer to the virtual environment where correspondence and other acts are all taking place while Information Technology is intervening. Physically, cyberspace cannot be located. It is made up of immaterial items like your website, blog, social networks, email addresses, private information, and renown. Cyberspace can be compared to a global electronic city with quick communication and no physical barriers.

Cyberspace is the digital platform used by PC organisations. It is a place where people can communicate, exchange ideas, share information, provide social assistance, run businesses, give orders, create inventive media, have fun, engage in political discourse, etc. [13] Cyberspace, the new frontier, is part of humanity's natural heritage, but regrettably some people misuse it, making it a new frontier for criminal activity of all kinds. It is now used to depict anything

[12] Jyoti Ratan, Cyber Laws & Information Technology,(48), 2014.
[13] Anirudh Rastogi, Cyber Law- Law of Information Technology and Internet,(2), 2014.

having to do with computers, information technology, the internet, and other web cultures. The term "netizen" refers to those who use the internet, and it is a combination of the phrases "web" and "resident." Therefore, the term "Netizen" refers to anyone who uses computers, information technology, or the Internet.

Early Concept of Crime:

Since the fall, man has been associated with crime and responsibility. Even as it advances, wrongdoing is still sneaky and always tries to remain undetected. Depending on their propensity and scope, many nations have used different approaches to combat wrongdoing.161 The obligation of the family was historically considered to be much more solidified than that of the community, the harmed party and his fellow could retaliate for some unacceptable by confidential retribution and self-readdress, and the plan of action to legal cure was simply seen as a discretionary option to self-change.

Modern Concept of Crime:

The current method of combating crime is effective. The arrangements of wrongdoing in contemporary culture have changed, especially in the information society, due to logical turn of events, modern insurgency, refinement of political establishments, schooling and scholastic edification of the individual, the slackening of strict hold over society, and the blurring of moral standards.

The law is Dynamic in character, so always showing signs of change, adding new crimes to the inventories and adjusting, changing and canceling previous ones. There have been astonishing changes in the space of crime. All around the world the changing idea of wrongdoing is rely on the development of the people in the public arena. In various nations, the idea of wrongdoing shows up in various lights at various times on the grounds that wrongdoing in one nation may not be a wrongdoing in another and a wrongdoing at one time may not be wrongdoing at another as well as the other way around."

Criminal Liability is Cyber Crimes:

Mens rea and actus reus are the two elements of crime, as stated clearly by the concept and nature of crime. Just actus reus is sufficient to compel criminal culpability for crimes against the state, such as fabricating evidence, forging money, committing middle-class crimes, and so forth. Under the criminal regulation it is the overall rule that an individual can't be indicted for a crime except if it is demonstrated for certain by the indictment and his act or exclusion is restricted by the criminal regulation. On the off chance that he possessed a character standpoint similar to the offence committed, the person is accountable for the equivalent. In addition, it is believed that actus reus without mens rea does not constitute a crime, and vice versa.

It is quite difficult to prove the two elements of crime in the event that cybercrime occurs. Cybercrime's actus reus is incredibly distinctive and diverse. For instance, there is the presence of actus reus in cyber space, which the law needs to govern, when someone starts using a PC with the aid of a console and mouse and tries to access information on another person's PC without his consent.

A debate about whether another law is necessary to deal with this new kind of guilt has been sparked by cybercrimes. There is a school of thought that holds that cybercrimes are really no different from common crimes like trespassing, burglary, or fraud with the exception that a PC was used as the means or instrument of the crime. The request school places a lot of emphasis on the extraordinary characteristics of emerging innovations and exceptional arrangements of challenges that are opaque to the current criminal law, such as the type and scope of cybercrimes, the strategy and difficulty in identifying the perpetrator, and the scope and demand. It fights that a new thorough regulation is expected to manage cybercrimes. [14]To control the cybercrimes two procedures can be embraced first and foremost, PC crime should be drawn nearer as both as customary crime and current crimes carried out through utilizing high technology computers and furthermore, PC crime should be drawn nearer as a crime which is one of a kind naturally for which new legal framework is required.”

Differential Association Theory:

This theory is based on the idea that, as Edwin Sutherland depicted in his 1947 book "Standards of Criminal science," modern society comprises a variety of competing norms and behaviours. This theory primarily deals with the conflicting interpretations of appropriate behaviour that contribute to a few crimes. Through communication with others, people become proficient in a particular manner of acting, whether it be criminal or sober. At the point when they gain criminal way of behaving from theirpersonal gatherings through correspondence they by and large utilize something very similar and along these lines perpetrate comparative crimes. This

[14] Parker, *Computer Abuse Research Update*, 2 Computer Law Journal, 329-352 (1980).

hypothesis contends that people primarily pick up on the traits, mindsets, behaviours, and cognitive processes involved in criminal behaviour through interaction with others. This theory focuses on how they learn how to commit crimes and profoundly examines conceptions of abnormality.

Factors responsible for Cyber Crime:

People are defenceless against crimes that are against the law, hence laws are supposed to protect them from such crimes, according to Professor H.L.A. Hart in his outstanding work "The Concept of Law." While PC frameworks are high-tech devices, they are really powerless when applied to the internet. Without much of a stretch, this technology can be used to fool or take advantage of a person or his PC through illicit or unauthorised access. The damage done to the victim as a result of the misuse of PC frameworks may have been direct or indirect. online criminals enjoy their crimes across networks unabated without fear of being caught and pursued for the crime they did because there is no sign of the foolproof component to secure and shield honest PC clients from online guiltiness.[15] Coming up next are the factors liable for the rise of cybercrimes."

The main factor contributing to the rise in cybercrimes is the enormous information storage limit. The PC has the capacity to fit an enormous amount of information on a little surface. In a disc ROM, a tiny CPU may store millions of pages. The information stored in ROM will constantly stay protected and not annihilated regardless of whether the power is switched off. A cybercriminal can purposefully get the enormous size of mystery or official information from the other individual PC inside a couple of moments. This prompts expanding cybercrimes."

Due to the complexity of PC frameworks, which are built from millions of lines of code, the second factor to blame for the surge in cybercrime is their use. Due to the dubious concept of the human brain, there is always a chance for a slip-up during every phase of handling. Cybercriminals are constantly ready to take advantage of these openings to elude detection and get access to the PC system. These criminals are referred to as programmers in the cyberspace who try to exploit flaws in current operating systems and security tools.

[15] H.L.A. Hart, The Concept of Law, (73) 2012.

Amendments in Bharatiya Nyaya Sanhita, 2023 by the Information Technology Act, 2000 (Previously IPC, 1860)

The enactment of the Information Technology Act, 2000 prompted substantial amendments to the then-existing Indian Penal Code, 1860, which have now been carried forward and updated within the framework of the **Bharatiya Nyaya Sanhita, 2023 (BNS)**. These changes align India's criminal law with digital advancements, particularly in the context of **electronic records**.

Section **29A** of the IPC, which defined "electronic record", finds its contemporary equivalent in **Section 2(1)(e)** of the BNS, where definitions are consolidated. Similarly, the concept of “documents” under **Section 29** of IPC is now reflected in **Section 2(1)(f)** of the BNS.

Under **Section 167 IPC** (now **Section 110 of the BNS**), public servants who prepare or translate false documents were made liable for similar actions involving **electronic records**. The updated provision ensures that framing a false electronic record with the intent to cause injury is punishable in the same manner as for physical documents.

Section 172 IPC, which penalized absconding to avoid summons, and **Section 173 IPC**, which dealt with preventing service of summons, now correspond to **Sections 228** and **229** of the BNS. These provisions have been extended to include failure or obstruction involving **electronic records**, thus reinforcing judicial processes in the digital age.

Similarly, **Section 175 IPC**, which criminalized the failure to produce documents before a public servant or court, is now aligned with **Section 230 of the BNS**. This section now also applies to individuals who fail to produce **electronic records**, emphasizing the evidentiary status of digital documents.

These amendments reflect India’s commitment to harmonizing its criminal justice system with the realities of the cyber era, ensuring that **electronic records are treated with the same legal weight** as traditional physical evidence.

Cyber Crimes in USA; Legislative and Judicial Approach:

"Mechanical advancements in communication have facilitated communication between people who lead very diverse lives. One of the most notable inventions in the communication space is the internet. The advent of the internet has transformed the entire planet into a global community. It has created a limitless virtual world that gives people sufficient opportunities to strengthen cross-border personal and professional interactions. The financial and social aspects of life have had a significant impact on globalisation since it began. The internet is a gift to human civilisation. The internet has connected people from every corner of the globe.

"The United States Defence Department started using a computer network in the 1960s, which led to the use of computer networks in academic and research institutions and the eventual development of the Internet Corporation of Assigned Names and Numbers (ICANN) and Protocol system in the United States. Any human endeavour that is successful leads to criminality, which calls for regulatory measures. Users should be reassured, law enforcement agencies should be empowered, and criminals should be deterred by legal provisions. As strict as its enforcement is, so is the law. In general, wrongdoing is not constrained by time, place, or a particular group of individuals.[16] Due to increased correlation in The internet encourages ethical, regular, and unlawful wrongs. Due of their internet usage, cyber users now have a new way to exhibit their criminal tendencies.

Because we are aware that cybercrimes are prevalent and have an impact on the entire world, all regional organisations and state governments have requested that legislators craft laws that address them. As a result, most countries started to do so. An effort has been made in this part to discuss digital legislation and to determine the role of the judiciary in combating these new forms of wrongdoing that are emerging in the US.

The Computer Fraud and Abuse Act (CFAA), 1986 was established by the congress as a modification to the existing computer fraud regulation (18 U.S.C. 1030), which states that an individual is at real fault for an offence on the off chance that he causes a computer to carry out any role with the goal of tying down access to any programme or information held in any computer or he accesses something that he means to get is not authorised; and he knows when he causes the computer. Unauthorised access to a computer or network without committing

[16] Success in any field of human activity leads to crime that need (delhicourts.nic.in)

another crime (such as obstructing system operations or obtaining secured data) is in essence illegal when it comes to computers used solely by the US government. Unauthorised access to any remaining computers, such as those used by the national government and others, including those that contain records relating to public safety and those that contain financial and credit information, requires additional proof of harm before criminal penalties take effect.

“The Data Protection Act, approved in 1998, regulates the use and capacity of personal information or data relating to people. Under the Demonstration, if any person intentionally gained access to a PC without authorization or in excess of that authorization, and through that access obtained data that was not fully resolved by the US Government in accordance with a Chief request or resolution to require assurance unapproved divulgence due to public security reasons or, on the other hand, unfamiliar relations, or restricted information, as described in the section of the Nuclear Energy Demonstration, knowingly transmits, transmits, sends, or causes to be transmitted, or attempts to transmit, transmit, communicate, or cause to be transmitted, something very similar to anyone not authorised to receive it, or obstinately holds something similar without transmitting it to the official or representative with reason to believe that such data so obtained could be used to the detriment of the US or to the advantage of any unfamiliar country.

Comparative Study of Cyber Crimes; Indian & USA Perspective:

The cyber world is a fusion of computers and various forms of correspondence. 1 The introduction of the internet has made the entire planet a global village. It has created a limitless virtual universe that gives people ample opportunities to strengthen both personal and professional connections across borders. The rise of globalisation has had a profound impact on both the financial and social facets of life. The advent of the internet has been a gift to society. The primary goal of the Internet is to connect people worldwide who have a desire to learn about the irreplaceable human instinct that led to the discovery of the cyber world.

“In 21st Century the social orders are progressively getting changed into information Social orders and their occupants into Information Organizers who are more educated regarding the occasions happening locally and internationally. Their activities depend on major areas of strength for the underpinning of information which is general, unbiased, convenient and recovered from different sources. People groups are becoming more aware of their liberties and open doors as a result of this upheaval, and computer, internet, and information technology are solely responsible for this progressive transformation. The way that people communicate and collaborate with one another throughout the world has evolved as a result of globalisation in the 21st century, and electronic correspondence is replacing earlier correspondence that was paper-based.

“Comparatively few organisations have identified coordinated cybercriminal organisations as their greatest potential threat to cyber security, and they are ready to protect themselves from such risks. Information technology is a two-sided coin that consistently brings us benefits and drawbacks. The rising open doors for productivities, productivity and worldwide correspondences acquired extra clients droves.[17]

The new media that has suddenly attacked humanity does not distinguish between good and evil, between local and global, between just and unfair, but rather provides a platform for the activities that take place in human society. Regulation, which controls how people behave, has a presence in cyberspace and is making an effort to adjust to its difficult issues. For a while, safety and well-being were only concerns with regard to insurance against threats from the outside world. 'Cyberspace' began to take shape nearby the oldworld at the turn of the century. As this new world becomes more and more intertwined with the old, disconnected one, cyberspace security has become crucial for a functioning society. A safe cyberspace implies a cyberspace where (and from where) no crime is committed. [18] For a thorough and organised comparison study, there are several aspects in cyber regulation that need to be determined.

Conclusion:

"Since the 1990s, cyberspace has rapidly and dramatically altered social orders, outpacing general sets of rules, the fair application of equality, and correctional procedures. The history of cybercrime might be described as being brief but extremely significant. As a matter of fact, there are different viewpoints on the veracity of the existence of this new breed of crime. Some claim that the development of the PC coincided with the invention of the first calculator because people began using machines for illegal reasons. As a result, some claim that cybercrime has been from the beginning of time. In reality, the history of cybercrime started

[17] R.C. Mishra, Cyber Crime: Impact in The New Millennium, (53) 2002.
[18]https://cybercrimejournal.com/.

with programmers who initially tried to break into PC networks just for the adventure of getting to high-level security organisations or to obtain sensitive or got information for personal gain or retaliation. It has been correctly said in criminology that a crime will occur whenever and whenever the open door benefits itself. Prior to this, the only kind of crimes that were commonly known to us were homicide, assault, burglary, blackmail, theft, dacoity, and so on. However, new types of crimes like hacking, cyber porn, cyber criticism, and so on now exist due to the evolution of science and technology, including PCs and web offices. 'Cyber Crime' is a misnomer. There is no distinction between a crime committed in the real world and a crime committed in the computer system because cybercrimes are only crimes that can be proven to have taken place. Just the way crime is committed has changed.

There are "no cyber-borders between countries" and these are "global" or "transnational." The terms "PC crime," "cybercrime," "e-crime," "hey tech crime," and "web crime" are interchangeable and often refer to crimes committed online using a PC or other organisation as a source, target, or tool. In the USA and the UK, there is no official definition. Unusually, neither the Information Technology Act of 2000 nor this definition of a "cybercrime" or "cyber offence" are used in India. The Information Technology (Amendment) Act of 2008 amended the Indian Correctional Code of 1860, yet despite this, it never uses the phrase "cyber crime."

Cybercrimes are discrete in nature and can be committed in the safety of one's own home without having to introduce themselves to the victim and without any actual eyewitnesses. Because a cybercriminal silently commits the crime without making much noise or showing any fear of being caught in the act, there are no signs of physical brutality or cries of agony at the time such offences are committed. These crimes can be perpetrated by a single person using a mouse click without knowing who will be the victim. In the majority of cases, the victim of these crimes won't even acknowledge what has happened to him, who committed it against him, or when it was carried out. Due to the lack of compelling procedures to identify cybercriminals both globally and at the public level, it is quite challenging. Various arguments have been made on the progression of cybercrimes. However, the emotions are in opposition to one another. First and foremost, any activity that occurs in cyberspace should be condemned and classified as a cybercrime. Additionally, many cybercrimes result in both the victim's computer and the perpetrator being killed because, in today's technological age, the majority of people are unaware of the types of crimes that fall under the category of cybercrime. Additionally, the US has not classified cybercrimes according to any conventional categories.

Cybercrimes are divided into three categories under the PC Abuse Act of 1990 in the UK, and the Information Technology Act of 2000 in India. Because there are no effective definitions of these crimes that are widely accepted or available, these crimes are growing more and more.
"In India, the IT Act is regarded as the primary cyber law because it is the as-it-were information technology regulation that devotes itself entirely to the electronic situation, including e-exchanges, internet business, e-administration, and so forth, with cyber-crimes gradually covered as well. The Indian Evidence Act of 1872, the Brokers Book Proof Demonstration Act of 1891, and the Hold Bank of India Act of 1934 are only a few of the present legislation that the Information Technology Act amends. 2008 saw its correction as a result of various gaps. Whatever the case, cybercrimes remain a problem, and it has been noted that this resolution's implementation has lagged behind its paper counterpart. The reason for this, according to the explanation, is that judges, examiners, examiners, and attorneys have difficulty comprehending the resolution's extremely technical language. The IT Act, 2000 was created to promote online commerce, however it hasn't been particularly effective in combating some other emerging cybercrimes. The absence of comprehensive cyber regulation and its adequate authorisation to combat cybercrime is the source of these crimes.

It is also giving the impression that part 66 A was incorporated with the intention of protecting the individuals' notoriety and preventing the exploitation of the organisations. However, the terminology used in the aforementioned portion goes well beyond the reasonable restrictions that could be imposed on free speech under Article 19(2) of the Indian Constitution, which could affect the unassailable fundamental right to free speech in person-to-person communication media. The notion of the offence is cognizable under section 66A, and the police specialists were initially hired to capture or conduct research without warrants in light of charges filed under the portion. This would result in a string of heavily publicised arrests of locals for publishing dubious content online, where the'shocking' contents were typically divisive political viewpoints. Most experts disregarded the warning that the Focal Government issued in January 2013 that no captures under Section 66A were to be performed without prior approval from a person who was not a member of the Monitor General of Police. The Hon'ble High Court proclaimed segment 66 An as unlawful and against the the right to speak freely of discourse and articulation and struck it down in ***Shreya Singhal and others v. Association of India*** since this segment had been profoundly abused by police in different states to capture the blameless individual for posting basic remarks about friendly and policy centered issues on systems administration locales.”

The **2011 Information Technology (Intermediaries Guidelines) Rules** have also received criticism based on a specific premise. These guidelines weaken the exceptions provided under the law, which released intermediaries from responsibility in certain circumstances and were found to encourage intermediaries to monitor content and implement online restrictions. In addition to these guidelines, the Information Technology (Method and Protections for Impeding for Access of Information by Open) Rules, 2009 allow for impeding that is perceived as concealed and fail to fulfil Protected shields of typical equity. The use of information technology by the fear-based oppressors in the public sphere helped them use it as a tool and a focal point to achieve their goals. One of the most perplexing national and international issues of our time is cyber psychological oppression, in which one country uses information technology to attack other nations. This phrase is still not defined by the IT Act. Global psychological militants use websites, such as those of Al-Qaida, to launch attacks. These websites have links to Osama Bin Laden. The loaded attack on the Indian Parliament on December 13, 2001, the attack on the WTO and Pentagon on September 11, 2001, the email threat to attack the Indian Parliament and US office on December 16, 2005, the attack on the American Information Focus in Kolkata by Aftab Ansari from Dubai, and Dawood Ibrahim's fear-based oppressor activities are all examples of cyber illegal intimidation, also known as cyber war or net conflict.

"In India, there are remarkably fewer prosecutions because to the corporate sector's reluctance to disclose cybercrimes out of fear of negative publicity, which leads in fewer legal professions. Due to a lack of information and heightened people's awareness, the majority of occurrences are not reported. This encouraged online criminals to commit these kinds of crimes. These crimes are a result of the lack of multiple-danger security systems, technologically based projects or camps, and associations' rejection of foolproof PC techniques at the local and international levels.

Although it is likely that the Indian regulatory and legal authorities play a significant role in combating various types of crime, there are times when it appears that the legal framework is insufficient to address the threats posed by cybercrime, which has emerged as a threat to fundamental rights. Due to inadequate legislation and a lack of legal responses to cybercrimes in India, the country's legal system would likely face challenges in the not-too-distant future. Additionally, it has been discovered that the decisions and actions taken by the police to investigate cybercrimes are almost always slightly wrong. Because if law enforcement makes a mistake in this situation, a nice resident may still be affected. Due to the US laws and standards' easier accessibility and wider application throughout the world, the Indian legal system may be persuaded to follow the guidelines established by US courts.

The administrators' inability to keep cybercrime regulation in advance of the swift mechanical curve has occasionally perplexed the police. In the event that such a situation arises, lawmakers will have to decide how to balance competing demands for individual liberties like security and free speech with the need to preserve the integrity of public and private networks worldwide. It is also discovered that the investigating offices and regulation authorization agencies are currently using the same techniques for acquiring, studying, and evaluating the evidence while investigating cyber-crimes as they do in cases of traditional crimes. The fact that certain offences under the IT Act are cognizable and subject to bail would allow the police additional latitude to take action. The current situation resulted from a lack of proper jurisdictional regulation, cyber courts, and legitimate specialised training to examine officials, investigators, judges, and promoters both at the public and global level.

Both cybercrime and real problems are global in scope. The G-8 Gathering, OAS (Association of American States), APEC (Asia-Pacific Monetary Collaboration), and the Gathering of Europe are just a few of the international organisations that have made numerous efforts to ensure the harmonisation of arrangements in individual countries. However, this methodology is seen as crucial in the analysis and arraignment of attacks against the core of PC systems and organisations. Due to the nature of cybercrime, any cybercriminal can commit a crime from anywhere in the world. There is a strong requirement to visit the victim location in order to commit a crime against him. There is a lack of the universally applicable legal system that should be implemented, supported by specialised and well-prepared law enforcement, and appropriate general awareness.

Towards the conclusion, it is highly likely that it will be implied that information technology and the internet have become an essential part of our daily lives in the modern world. We use the internet and technology for each cause. We can't imagine living in the modern world without the internet. It seems likely that it won't slow down very soon and will keep developing until fresh methods of combating it are offered. Since science, modern technology, and the internet have created a new virtual paradise for people of all kinds to join and communicate with, different societies and sub-societies. But when the internet falls into the wrong hands or is used or restricted by individuals or groups with filthy dispositions and vengeful intentions, it will eventually be a virtual purgatory for everyone. Due to the usefulness of information technology and the internet, cybercriminals and psychological militants used PCs as targets or tools for these kinds of crimes.