International Scientific Journal of Engineering and Management ISSN: 2583-6129
Volume: 03 Issue: 04 | April – 2024 DOI: 10.55041/ISJEM01520
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

CYBERCRIMES, LAW, AND CYBER FORENSICS: COMPARATIVE STUDY OF INDIAN, BRITISH, AND AMERICAN CONTEXTS

Sayed Aheed, LLM (Business Law),

Amity Institute of Advance Legal Studies, Amity University

ABSTRACT

New forms of crime have emerged with the rising prevalence of computer misuse. Some of them include the use of cutting-edge tools and methods for criminal conspiracy. From spreading fraud through email to stealing and reselling intellectual property, cybercrime covers a lot of ground. The domain of computer science known as "cyber forensics" is considered to be among the most essential subfields. It is concerned with the investigation of cybercrime. The concept of cyber forensics is broken down into its parts by the author in this paper. This paper focuses on the significance of the topic as well as some of the methods and instruments that are used by cyber forensic investigators. The objective of cyber forensics is to conduct an examination of electronic content in a manner that is forensically sound with the goals of preserving, recovering, analyzing, identifying, and presenting facts and views about digital information. Cyber forensics evidence undergoes the same processes as other digital evidence and serves as supporting evidence in judicial proceedings. Cyber forensics is often linked to the investigation of cybercrime, but it may also be utilized in legal actions involving private parties. This paper demonstrates the necessity for further investigation into how cyber forensics might be used to enhance the identification of cybercrime. This research will help fill in some of the gaps in our knowledge of how cyber forensics investigations are conducted in India and explore cyber security policy in the United Kingdom, the United States, and India to identify both similarities and differences.

Keywords: Cybercrime, Cyber Forensics, Policy

INTRODUCTION

The increasing need for massive data storage is driven by the exponential expansion of the Internet. With the proliferation of personal computing devices like smartphones, the number of cybercrimes committed is on the rise. Hacking, bank fraud, and email spamming are just some of the many crimes that may be examined by digital forensics and cyber forensics.

Cybercrime means any illegal activity that involves the use of the Internet or any other electronic means to disrupt the normal operation of a computer or computer network. The computer may or may not have played a significant role in the conduct of the crime, but both the computer and the network are involved. Technology has given rise to a new genre of criminal activity: cyber-crimes. Cybercrime refers to any kind of criminal activity involving the electronic processing and transfer of data that occurs inside a computer system.[1]

To be more specific, illegal use of the Internet is what is meant by the term "Internet crime," which is a subset of cybercrime. Since computers and also the internet is used in almost every aspect of modern life (banks, communications, travel, healthcare, entertainment, etc.), this kind of crime has exploded in recent years. The problems associated with this sort of crime, such as hacking, intellectual property theft, pornography, child grooming, etc., have recently risen to the forefront. As technology has progressed, however, the scope of this kind of crime has expanded. The potential to participate in espionage, money theft, and other cross-border crimes, commonly referred to as cyber warfare, is growing in relevance for both state and non-state players on a worldwide scale. The International Criminal Court is one of the few institutions aiming to address this issue by bringing those responsible to justice for their crimes. When private information is unlawfully or accidentally captured, published, or leaked, it creates privacy issues.[2]

Many modern electronic gadgets, including storage devices, PDAs, and video game consoles, can receive data from the user, transmit it somewhere, and store it. This information or the use of these tools is the foundation of cyber forensics. Collating, analysing, and reporting digital evidence in a way that complies with the law is known as cyber forensics. It may be useful in cases involving forensic evidence, such as those involving the identification or prevention of criminal activity. Forensic cyber investigation extends beyond the data collecting and storage methods typically used by end users and IT support personnel. Like traditional forensics, cyber forensics is essentially the study of how the law may be applied to

[1] Dr. R. K. Chaubey, “An Introduction to Cyber Crime & Cyber Law” (Kamal Law House Kolkata) (2008).
[2] Vakul Sharma, “Handbook of Cyber Law” (Macmillan) (2002).

computer technology. Preserving, identifying, extracting, and documenting evidence from cyberspace is the domain of cyber forensics. The precision of evidence retention and the accuracy of data processing outcomes are paramount in cyber forensics, as they are in many other forensic disciplines.

HISTORICAL BACKGROUND OF CYBER FORENSICS

"Crime by Computer," written by Donn Parker in 1976, is widely regarded as the first depiction of the use of electronic information in the investigation and prosecution of computer-aided crime. Most systems were not heavily networked to the outside world; therefore, it was the responsibility of system administrators to ensure the safety of their systems. Audits of the system were developed to check the precision and economy of data processing, a costly endeavour back in the day. This auditing process amounted to the first-ever comprehensive attempt at ensuring computer safety. The outcome of these efforts was the ability to utilize audit data in investigations of possible malfeasance. Ad hoc organisations of volunteer law enforcement officers were formed by agencies including the Department of Defense, the Internal Revenue Service (IRS), and the Federal Bureau of Investigation (FBI), and given basic training on mainframe and mini-computers. These cyber forensics experts would aid other case investigators in retrieving information and accessing records from mainframe systems. In most cases, detectives with computer expertise would team up with network administrators.[3]

It was largely due to the fact that law enforcement and military investigators in the United States saw that criminals were becoming more sophisticated than the profession got its start. In the case of a suspected breach of security, govt employees tasked with guarding sensitive, top-secret information conducted forensic investigations to not only determine the nature of the breach but also provide insight into how such breaches may be avoided in the future. Eventually, cyber forensics, which investigates and responds to high-tech crimes, and the information security sector, which safeguards data and assets, merged into a single discipline. Over the following several decades and up to the present, the discipline will continue to develop. Both public and commercial institutions have started to do the same thing, either employing dedicated cyber forensics and information security experts in-house or, failing that, sometimes outsourcing such tasks to specialists. The necessity for cyber forensics studies in civil law disputes was recently recognised by the private law sector, leading to a boom in the area of rediscovering.[4]

[3] Dr. Vishwanath Paranjape, "Legal Dimensions of cybercrimes and Preventive laws," Central Law Agency (2010).
[4] Dr. Amita Verma : Cyber Crimes and Law (Central Law Publications) (2009).

ISSN: 2583-6129
DOI: 10.55041/ISJEM01520

By the middle of the twentieth century, specialised blood tests had been developed alongside methods for analysing urine, saliva, and other bodily fluids. As a field, cyber forensics can be traced back to 1984, with the creation of the FBI's "Magnetic Media programme", which would eventually become known as "the Computer Analysis and Response Team (CART)". The International Association of Computer Investigative Specialists (IACIS)" was founded in 1988 as a non-profit organisation with the mission of educating and certifying computer forensic experts worldwide. After this, in 1995, the "International Organization for Computer Evidence (IOCE)" was formed to facilitate communication and collaboration among groups working with electronic evidence and to guarantee uniformity and quality in the forensics industry. With the rise of cyberattacks, the Group of Eight nations decided in 1997 that "the law enforcement officers must be taught and equipped to cope with it," emphasising the necessity of cyber forensics. The Group of Eight tasked IICE in 1998 with developing standards for digital evidence around the globe. In the same year, INTERPOL had its Forensic Science Symposium. In the year 2000, the FBI opened its first regional cyber forensics laboratory in San Diego.[5]

WHEN AND HOW CYBER FORENSICS IS USED?

Evidence on a computer may be collected and preserved with the help of cyber forensics, an area of technology. Cyber forensics is often used to unearth material that may be presented as proof in a legal proceeding. There are many fields outside of law enforcement that fall under the umbrella of cybersecurity. Professionals in this industry may sometimes be asked to rescue inaccessible files from dead hard drives, broken servers, or wiped operating systems.

An integral part of contemporary investigations may involve cyber forensics. After a crime has been committed, one of the first places investigators seeks evidence is the suspect's electronic devices, such as their computer or mobile phone. A specialist in cyber forensics might be helpful in this situation. When a suspect is located and their computer or phone is seized as evidence, a cyber forensics expert will examine the device for any clues that can help with the investigation. They must adhere to stringent protocols while researching to provide admissible evidence. Whatever they find—papers, history of sites visited, or even metadata—could be utilised as evidence in a case against the accused.

Professionals in the domain of cyber forensics are not limited to only gathering evidence; they may also engage in data recovery. Experts in cyber forensics can recover data from damaged hard drives, crashed

[5] *Ibid*

ISSN: 2583-6129
DOI: 10.55041/ISJEM01520

servers, and other systems. Outside of finding criminal evidence, this is helpful for anybody who has lost critical information, such as firms that have suffered a system meltdown.[6]

The goal of cyber forensics is to piece together what occurred, who was involved, and when it happened by examining data generated by or stored in computer systems. This procedure locates, retrieves, examines, and stores electronically stored material for future retrieval and potential use as evidence in court proceedings.

Examples of common situations in which cyber forensics is used include:

- A data breach occurs when sensitive company data is leaked either accidentally or maliciously.
- Theft of intellectual property occurs when an employee either gives stolen information to a rival firm or utilizes that information to start a business that competes with the victim.
- Instances when an employee breaks the rules regarding the usage of computers and the Internet. Some businesses have policies about acceptable computer and Internet usage. Cyber forensics may assist establish the timeline and circumstances of any illicit conduct that may have occurred on company computers.
- Evaluation of losses sustained after an occurrence.
- White collar offences. These crimes are perpetrated by the government or commercial officials who are not motivated by violence but by money. Identity theft, Ponzi schemes, and advance fee fraud all fall within this category. The losses from white-collar crimes may be catastrophic, including the loss of a person's life savings, the collapse of a business, or the loss of a fortune for investors. Investigating these types of crimes may be aided by cyber forensics.
- To obtain an advantage, the cheater willfully provides inaccurate or misleading information. Cyber forensics may aid in the investigation of fraud committed online or with the use of technology.
- Inappropriate touching, lying, and being careless with women.
- The gathering of evidence might one day lead to the dismissal of an employee.
- Common law and civil litigation. The reason for this is that some criminals keep files on computer systems.
- Commercial enterprises may also benefit from cyber forensics in the event of intellectual property theft, forgeries, employment disputes, bankruptcy investigations, or fraud compliance.

[6] John N, "Developments in Information Technology | by Niya John | Medium" (Medium, March 6, 2018) <https://medium.com/@niyajohn9495/developments-in-information-technology-b93c74b7bd79> accessed April 22, 2024

Acquiring and processing the evidence appropriately is essential for its admissibility in court in any of these situations. This is the only way the data may be used as evidence in court, whether to prove or disprove allegations.[7]

CYBER FORENSICS INVESTIGATION AND DIGITAL EVIDENCE

Forensics is the art and science of discovering ideas, extracting and conserving them, and presenting them in a court of law. The first step in cyber forensics is to evaluate the occurrence, analyze the method of operation behind the crime, and make a list of all conceivable locations where the evidence could be found. Computer (disc) forensics, mobile forensics, network forensics, and so on are all part of cyber forensics. Digital forensics is divided into four stages. Some of the work completed may overlap between phases, but they are extremely different:[8]

- Collection
- Examination
- Analysis
- Reporting

Forensic analysis of data storage devices must be performed using software tools for undeleting deleted files, breaking passwords of secured files, decrypting encrypted information, and so on. The leading tool is 'Encase'. Thus, Cyber Forensics includes:

- Outlining the source of the email.
- Finding and decrypting password-protected information.
- Recovering deleted data.
- Careful identification and classification of all items including cables, peripherals, and external storage media.
- Noting the time shown on the computer's built-in clock
- Video graphing the computers where they are now located, paying close attention to the wiring of any add-ons and extras

[7] "When Would Computer Forensics Be Used? | Computer Forensics NZ" (*Computer Forensics NZ*, September 11, 2021) <http://www.datarecovery.co.nz/forensic-investigation/when-would-computer-forensics-be-used> accessed April 22, 2024.
[8] DR. Faizan Mustafa, "Challenges of Internet, Cyber-sex and Muslim Youth: need for an Islamic Solution," Aligarh Law Journal (1998).

- Appropriate events for safe shutting down of machines that are operating at the time of the attack.

eDiscovery refers to the process of exploring potential solutions for a company. Legal standards for the administration and admissibility of electronic discovery evidence must be satisfied, and the process must be repeatable and standardised. For instance, e-Discovery may benefit from the addition of email archiving. A discovery process that can stand up in court can be repeated with accuracy, provides sufficient information, and complies with all applicable laws and regulations regarding the handling and admissibility of digital evidence. Finding, collecting, preserving, processing, examining, and producing relevant material stored electronically are all part of a successful e-discovery process.[9]

When a hard disc has to be analyzed for suggestions, there could be inadvertent data corruption or an allegation of data manipulation. As a result, the investigator does no forensic analysis of the original hard disc that he has confiscated. The investigator typically builds a clone of the detained hard disc, which is a bit of an Image Copy of the suspicious disc, and analyses it. The duplication is carried out in the presence of witnesses, preferably the hard disk's owner. For each questionable disc, at least two cloned discs are generated; one is returned to the disc user, while the original is sealed for submission to the Court. It should be noted that even deleted data can be read by scientific software capable of reading binary data at the byte level. Even when a disc is reformatted using high-level formatting, the data is not destroyed and is thus retrievable.[10]

Volatile Data

Volatile data is data that is used by the computer while it is turned on and then discarded when the machine is turned off. It is normally stored in RAM (Random Access Memory) space. Needless to say, before shutting down the computer, an investigator should try to understand what is in volatile memory by using tools that swiftly analyze RAM. Analyzing RAM may shed insight into previous and current network associates, which is crucial when determining the remote destination with whom the malware is connecting, the source of child pornography, and so on. 'Mem Marshal 1.0' is a popular forensic application that supports RAM examination in Windows XP computers.[11]

[9] Cyber Crime - A challenge to Forensic Science, B.B. Nanda 8s Dr. R.K. Tewari, the Indian Journal, pg. 102 to 103 (April – September, 2000).
[10] Cyber Crime Investigation 8s Prevention, A.S. Chawla, ISP, the Police Journal, April-September (2016).
[11] M.K. Nagaraja, “Cyberpom Crimes: an analytical approach to investigation, The Global Threat of Software Piracy,” CBI Bulletin. (July 2010)

ISSN: 2583-6129
DOI: 10.55041/ISJEM01520

Investigate and analysing databases and their information is the subject of database forensics, a branch of cyber forensics. Forensic database analysis may make use of row-level timestamps (update timings) in a relational table to verify the authenticity of user operations.[12]

Mobile Forensics

This comprises data extraction from SIM cards or data cards, as well as data extraction from mobile hardware, including erased data. A gadget like this is called 'Cellebrite.' SMS and MMS are important types of information obtained through mobile phones. Service benefactor logs and call data records are vital additional shreds of evidence that can be gathered. With the fast-paced field of GPS Forensics, Mobile Device Forensics, also known as “SatNav Forensics”, is a relatively young discipline. It is used to examine and analyse GPS devices to recover data such as Routes, Photos, Audio, TrackPoints, TrackLogs, WayPoints, and so on.[13]

IP Tracing

There is a plethora of software available that resolves IP addresses and also displays the typical flow of data via the internet. 'Trace Route' is a popular example of such a tool.

Network Forensic

This entails encountering digital evidence distributed across computer networks. Wireless forensics is a subset of the larger discipline of network forensics. Wireless forensics aims to provide investigators with the resources they need to capture and analyse data from wireless network traffic. The information gathered may be basic statistics or indicative of the broad use of Voice over Internet Protocol (VoIP) systems, especially those that employ wireless networking. One must be wary of the risks involved in gathering evidence through a network. Because of how rapidly logs may evolve, crucial data might vanish within seconds of beginning a log study. Getting evidence from some sources, such as internet service providers (ISPs), may need permission.

This process can take time, which increases the chances of evidence loss. Other pitfalls include the following:[14]

[12] *Ibid*
[13] *Ibid*
[14] *Ibid*

- A normal computer or network activity may seem like an attack to an investigator or system administrator.
- The continuity of signs may be broken at certain points.
- There is a chance that logs are unspecific, missing, or incomplete.
- Other countries may be engaged in the probe due to the global nature of the Internet. That might cause problems for the probe on the legal and political fronts.

Malware Forensics

It is concerned with the analysis and detection of malicious code to study their payload, viruses, worms, Trojans, key loggers, and so on.

Email Forensics:

E-mails, calendars, and contacts, even those that have been deleted, may often be recovered and analysed.
A typical forensic lab will consist of 3 important divisions:

- Data Acquisition Division- responsible for picking up sanitized hard disks for data acquisition and cloning the suspect hard disk into sanitized hard disks.
- Data Analysis Division- Analyses the data and makes reports

Data Custody Division-Responsible for storing the disk in a protected safe (free from external magnetic influences) and for transmission of disks in properly packaged condition to avoid corruption in transit.

COMPARATIVE ANALYSIS OF CYBER LAWS AND CYBER FORENSICS – UK, US AND INDIA

UK

In the UK, there is a lack of unified legislation addressing cybersecurity as a whole. The potential of civil actions under the common law serves as a foundation for the many statute-based laws that exist today. The “Computer Misuse Act of 1990 (CMA)” makes it illegal to tamper with a computer without permission; the “Investigatory Powers Act of 2016 (IPA)” makes it illegal to intercept communications, including communications sent or received by computers; and the “General Data Protection Regulation (GDPR)” makes it mandatory for organisations to take reasonable precautions to protect individuals' data. Important laws include the (GDPR), the “Data Protection Act (DPA) of 2018”, and the “Network and Information Systems Regulation (NISR) of 2018”; the “Fraud Act (FA) of 2006”, which makes it illegal

to commit acts that amount to fraud; and the "Intellectual Property Rights Enforcement Act" which makes it illegal to infringe on the ("the Copyright, Designs and Patents Act 1988").[15]

When it comes to cybersecurity, the primary focus of English law is on deterrence via punishment (most notably, the failure of data controllers and processors to keep personal data safe).

The General Data Protection Regulation (GDPR) applies to all companies, regardless of location, that target customers located inside the European Union (EU). This policy does not apply to processing carried out by a person in the context of his or her own home or household, or processing carried out in the interest of law enforcement or national security. In addition, anyone in charge of personal information must demonstrate compliance with seven privacy principles. The suggestions made by the Information Commissioner's Office (ICO) further on and clarify these principles. To put it bluntly, the ICO may slap you with a big punishment if you infringe any of these regulations. The regulator may seek criminal prosecution for DPA offences, and it has consulted on whether it should have powers under the Proceeds of Crime Act 2002 to prevent criminals from benefitting from data-related offences.[16]

The DPA expands upon, supplements, and offers exemptions from the GDPR. With few exceptions, the DPA makes it a crime to deliberately or recklessly access or disclose personal data without the agreement of the controller (blagging). It also controls how agencies like the Serious Fraud Office, Financial Conduct Authority (FCA), and National Crime Agency handle personal information (NCA).

It is a violation of the CMA for a person to cause a computer to perform any function with the intent to secure access to any programme or data held in any computer, or to enable any such access to be secured, if the access he or she intends to secure or to enable is unauthorised, and the person knows at the time that the function is caused that the access is unauthorised. Due to the extreme nature of the damage they inflict or the threat they represent to national security, several of these crimes may receive a sentence of life in prison.

There are a wide variety of methods for protecting data on a computer or inside the software. In the CMA, the word "computer" is not defined. Unauthorized access occurs when someone other than the person responsible for the computer and authorised to make such a determination gains access to the system.

[15] "Cybersecurity in United Kingdom (England & Wales) - Lexology" (*Lexology*) <https://www.lexology.com/library/detail.aspx?g=09262dc8-609b-45b1-bba9-8291f6d9c112> accessed April 22 2024
[16] *Ibid*

The CMA adds new offences when unauthorised access is used to commit other crimes like theft or fraud or to damage the functionality of a computer (such installing viruses or spyware). Ten years in prison is the maximum punishment for such an offence. It is also a crime under the CMA to purchase, manufacture, alter, provide, or sell anything that may be used to commit a crime under the CMA.

USA

No federal legislation in the United States addresses data security, privacy, or cybersecurity. In addition to the federal regulations, some states have passed cybersecurity legislation. As a result, there is a patchwork of federal and state rules that, depending on the kind of company, may have wildly different effects. More than a decade has been spent looking for a solution by both the government and private sector. American technology leadership and e-commerce have both contributed to a rise in cybercrime. It may have taken a while, but we've arrived. There has been an uptick in data breaches as a consequence of the effects of the digitalization of the financial sector, hospitals, and small and medium-sized businesses (SMEs).[17]

Due to the meteoric rise in the number of digital platforms, data breaches have taken on new dimensions since the start of this new digital age. Between 2005 and 2015, more than 500 million records in the United States were exposed due to data breaches. The United States had 1093 data breaches in 2016, leading to the loss of 36 million pieces of information.

These newly enacted and updated federal cyber security legislation are intended to strengthen existing federal policies in this area. Here are a few instances that illustrate this: Cybercrime poses real risks, and it's up to us as a society to make sure everyone knows how to be safe online. The spread of knowledge about cybersecurity threats and other difficulties is another goal.

It's possible that sharing information between private companies and the government is acceptable. The bill was originally submitted in July 2014, and it passed the Senate and was signed into law the same month. To improve cyber defences, President Obama signed the Cybersecurity Enhancement Act on December 18th, 2014. Efforts are being made by both governments and businesses to improve cybersecurity training and study for the public.

To educate citizens on the risks presented by businesses without adequate security measures, several governments have passed legislation. The Personal Information Protection Act of 2003 gives residents of

[17] EES, "Cybersecurity Laws and Regulations in US 2024 - EES Corporation" (*EES Corporation*, November 4, 2021) <https://www.eescorporation.com/cybersecurity-laws-and-regulations-in-us/> accessed April 22 2024

ISSN: 2583-6129
DOI: 10.55041/ISJEM01520

the Golden State peace of mind when it comes to the security of their private information. Companies are free to use their safety procedures in the case of a violation of cyber security laws. According to the concept, a company's reputation and financial losses may be avoided if it invested in cyber security.[18]

Other states have been inspired to follow California's lead because of the positive example it has established. New York City's Cybersecurity Laws for the Financial Sector Numerous factors pose a risk to an organization's IT systems. The DFS warns that the threat to data and financial systems from governments, terrorist organisations, and individual criminals is worse than it has ever been. Internet fraudsters have been actively searching for security holes via which they may access users' private data.

The consequences for criminals who get access to private data on New York residents and businesses might be severe. It will need a substantial amount of legislation to ensure that cyber security measures remain at their current state of effectiveness. By enacting this legislation, both IT companies and their customers will have their data safeguarded. A thorough risk assessment and plan for mitigating such risks are essential to meet this level. On March 1, 2017, new legislation governing cyber security in the state of New York went into effect.

The New York State Department of Financial Services' annual certification of compliance has been submitted. There is no more to tell; the last chapter has been written. In response to current cyber dangers, federal authorities have developed many steps to assist businesses in properly securing their data. Administration networks are vulnerable to hacking despite official attempts to prevent it. The same is true of non-public enterprises. The safety of a company's most vital records and software is a top priority. Every day, cybercriminals launch increasingly sophisticated assaults. The best business plan is the one that stops problems from ever occurring.

Important federal cybersecurity legislation includes the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and the Homeland Security Act. To meet all three of these conditions, businesses and organisations in the healthcare, financial, and public sectors must prioritise data and system security. In any event, it's not easy to say whether or not an adequate degree of security would work. All government agencies must apply FISMA's information security policies, principles, and standards.

INDIA

[18] "Homeland Security Act | United States [2002]" (*Encyclopedia Britannica*) <https://www.britannica.com/topic/Homeland-Security-Act> accessed April 22, 2024

Misleading someone about the origin of a communication by sending it over a single telecommunications network, delivering an improper message, or using a digital document are all examples of this type of cheating. trying to steal email signatures or identities, including using another woman's passcodes or authentication system, or gaining hijacked computer systems or other telecommunication technologies Criminal violations of Section 66 are cognizable, and the accused is not eligible for bail. Regulation 4 of the Reform Act makes it clear that violating Section 48 of the 2004 Law with malice aforethought or in violation of the law carries responsibility, and so may result in sanctions such as incarceration, fines, or both.[19]

With the passage of the Computer Crime Act in 2005, India's basic law was brought up to date. Under the definition of "technology" in the Indian Penal Code, digital recordings and papers are treated the same as physical documentation. Articles 194, 209, 464, 469, 467 through 471, 475, 477, 478, etc., which deal with the fraudulent entry in a register or wrong paperwork, have been amended to include the words "digital record and excel spreadsheet," bringing them within the jurisdiction of the IPC. To commit acts of forgery or fabrication of record keeping in a crime, it is now legal to use digital records and computer files instead of traditional paper records and paperwork. To ensure that the necessary paperwork and/or punishments can be protected and proven under either the IPC or the IT Amendment Act, investigating organisations must, per the aforementioned ordinance, file cases and charge sheets citing the relevant portions of both laws. In cases involving similar offences, this includes Sections 464, 467, 469, and 470 of the IPC, as well as Sections 43 and 69 of the IT Amendment Act. It was only possible to present physical evidence in court before the IT Law was enacted. The IT Law formalised the validity of digital documents and files. Section 68B of the Act, which codified the acceptance of electronic document authentication as evidence, was a ground-breaking reform. The term "papers" in the definition section of the Indian Evidence Act is expanded to encompass "any papers constituting digital records." Data, "digital certificate," "digital form," "secure digital document," and "digital signature" are all examples of terminology that were introduced to create the backbone of a Legislation's evidential relevance.[20]

Some of the cyber attackers of today aim their attacks to target the energy, communication, financial, and transportation sectors. According to CERT-IN, every 10 minutes, a new cybercrime was recorded in India last year. Authorities should work together to counteract this worrying trend. Once restricted to computer

[19] Madhyama Subramanian, "India: Promoting Internet Safety amongst 'Netizens'" <https://www.unodc.org/southasia/frontpage/2012/May/india_-addressing-the-rise-of-cybercrime-amongst-children.html > accessed April 22, 2024

[20] Dr. R. K. Chaubey : An Introduction to Cyber Crime & Cyber Law (Kamal Law House Kolkata) (2008).

hacking alone, cybercrime has recently expanded to encompass data theft, ransomware, child pornography, and many other forms of online wrongdoing. Crypto-jacking refers to the practice of secretly installing malware on a victim's computer for mining cryptocurrency without the user's knowledge. Some dangers that may occur on the web include information disclosure, industrial sabotage, and the loss of privacy through C&C IT transfers.[21]

CONCLUSION

To conclude, Since the growth and improvement of electronic systems are intrinsically linked to the long-term development of our society, we must endeavour to bring more attention to this issue. The battleground of the future will be the Internet. There has to be an international agreement on cyber deterrents, and all nations need to take the necessary measures to make that happen.

Future years will see an increased reliance on computers. Without a computer, we can't function normally in society. Because of this, we should expect a parallel rise in the crime rate as the number of people who utilise technology grows. Casework about cybercrime must be meticulous if the truth is to be uncovered. It is crucial to provide training for law enforcement and judges. When it comes to prosecuting incidents of cybercrime, India has a long way to go. Protecting practises related to prosecuting instances involving computer-based criminality is essential if we are to approach them with a military mindset. For deterrence purposes, the system must allow for severe punishment of computer crime and computer offenders. Most IT Act violations may now be prosecuted on a bailable basis, with maximum sentences of 3 years. This penalty has to be extended to a point where the offender is less likely to repeat the same or similar crimes in the future. For efficient tracking and documentation of computer cases, a separate bench composed of impartial members is required. The establishment of cyber judges allows law enforcement to demonstrate its competence in handling cybercrime matters.

[21] "Cyber Laws of India - ISEA" (ISEA) < https://www.infosecawareness.in/cyber-laws-of-india > accessed April 22, 2024