Library Progress International *Print version ISSN 0970 1052*
Vol.44, No.4, Jul-Dec 2024: P. 792-802 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Navigating The Legal Labyrinth: Framework And Challenges In Combating Cybercrime

Puja Gupta*[1], Dr. Baloy Bhattacharjee[2] Dr. Jayanta Ghosh[3]

[1] Researcher, Department of Legal Studies, Arunachal University of Studies, Namsai, Arunachal Pradesh. North-East Region of India, Email: pujaguptadigboi26@gmail.com
[2] Assistant professor of law at Arunachal University of Studies in Namsai, Arunachal Pradesh. North-East Region of India, Email: baloybhattacharjee@gmail.com
[3] Assistant Professor of Law, The WB National University of Judicial Sciences, India. Email: jayanta.crsgpp@nujs.edu
Corresponding author: Puja Gupta, Email: pujaguptadigboi26@gmail.com,
\

How to cite this article: Puja Gupta, Dr. Baloy Bhattacharjee, Dr. Jayanta Ghosh (2024). Navigating The Legal Labyrinth: Framework And Challenges In Combating Cybercrime. Library Progress International, 44(4), ***792-802***

ABSTRACT

This research delves into the intricate landscape of cybercrime, aiming to unravel the complexities of the existing legal framework while scrutinizing the formidable challenges inherent in combating this evolving menace. The study employs a qualitative and descriptive research approach to achieve three primary objectives. First, an exploration of the current legal framework surrounding cybercrime is undertaken to comprehensively understand the multifaceted dimensions of this regulatory landscape. Second, the study aims to better understand the challenges that law enforcement and cyber security authorities face when combating cybercrime. The study employs a multifaceted research strategy, incorporating legal analysis, case studies, and expert interviews to provide a holistic understanding of the challenges at hand. Third, the research engages in a rigorous analysis of potential solutions to these challenges, seeking to identify and evaluate effective strategies that can enhance the efficiency of efforts to combat cybercrime. This study's findings not only advance scholarly understanding of the legal issues surrounding cybercrime, but also provide practical insights for politicians, law enforcement agencies, and cyber security practitioners. By navigating the legal maze of cybercrime, this study hopes to pave the way for a more resilient and responsive legal framework in the face of an ever-changing digital threat landscape.

Keywords: Cybercrime, Challenges in Cybercrime, Legal Framework, Cybersecurity, Cyberattack

INTRODUCTION

Cybercrime is a serious hazard to both individuals and organizations in the current digital era. As a result of technical improvements and increased reliance on the internet, cybercrime has proliferated and is a significant problem for law enforcement organizations around the globe. Cybercriminals are always devising new ways to bypass security measures and steal sensitive information. These methods include ransom ware attacks, data breaches, phishing, and identity theft. Cybercrime is a broad phrase that refers to a variety of illegal behaviors, Examples include electronic cracking and denial-of-service attacks, in which computers or computer networks are utilized as a tool, target, or location for unlawful activity. It may also relate to more traditional crimes in which computers or networks facilitate unlawful activity. Cybercrime is one of the most serious dangers to the global economy, affecting both national and corporate interests. Cybercrime causes tremendous expenditures and losses for businesses. They include data destruction and corruption, money theft, intellectual property, financial and personal data, business interruption due to a cyber attack, reputational damage to the company, lost productivity, and so on. The fast growth of cybercrime necessitates the development of effective deterrent strategies (1).

History of Cybercrime

Many people wonder how cybercrime got started. This typically has to do with the development of the internet as well as computers and computer networks. Criminals spotted an opportunity as soon as it was widely acknowledged that computers retain valuable information. Before we talk about cybercrime, let's define crime: any act or inaction that compromises any legally protected social, political, moral, or legal interest is considered a crime and is subject to legal consequences. Participating in behavior that society has declared illegal because it jeopardizes the society's ability to uphold order is what constitutes "crime." Because cybercrime entails a number of unlawful actions that damage people, companies, and data, it also disturbs the status quo. Crime, such as murder, requires a weapon, and rape, for example, involves force; cybercrime, on the other hand, requires a computer. The word "cybercrime" has come to represent risk and insecurity on the internet and broadly refers to crimes that occur within that realm. Although the term "cybercrime" is relatively new—it first appeared in the 1960s— Tech enthusiasts may have developed the phrase "MIT," which refers to a train model whose operation has been tweaked.(2).

Cybercrime Definition

Cybercrimes include illegal computer system interference, acts that undermine the confidentiality, integrity, and availability of computer system data, as well as the exploitation of computer resources for terrorist purposes. They also include the misuse of computers for financial, political, or blackmailing purposes; the illegal interception of computer systems and data via computers is used to intercept networks and computers.

Numerous actions, including copyright disputes over the distribution of protected content, including books, music, videos, audio, and other economic and academic endeavors, are connected to cybercrimes in the social sphere (3).

Causes of Cybercrime

These days, cybercrimes are more common for a variety of reasons. The affordability and ease of access to computers, smartphones, and the internet may be some of these causes. Low-cost bundles provided by mobile phone providers. increased exposure of children and teenagers to information and communication technologies. Computer education is becoming a required course in all universities, colleges, and schools. The age range of people who use computers is growing. It is a truth, nevertheless, that many individuals use the internet without realizing the risks involved and end up being victims of cybercrimes. Hackers can quickly get access to computer systems' hard drives and other storage devices, allowing them to steal sensitive data and information. People are careless when it comes to safeguarding their smartphones and PCs. Businesses and the public do not want to invest money on system security (4).

Cybercrime Ethics and Legislation

A collection of morally sound guidelines is known as cyber ethics. Additionally, a code of conduct is determined by security protocols. There are several varieties of it –

Legislations to Combat Cybercrime

Most security specialists think that enacting strict laws against cybercrime might significantly aid in its fight. For instance, very few federal laws have been passed to combat cybercrime, such as the USA PATRIOT Act of 2001 (terrorism), the Digital Millennium Copyright Act (technology copyright protection), The Computer Fraud and Abuse Acts of 1986 and 2001 (computer threats), the National Information Infrastructure Protection Act of 1996 (criminal intent), and the Computer Security Act of 1987 all address federal information security issues. These laws have been utilised to prosecute cybercriminals who employ malware to steal the identities of unsuspecting victims.

Similar legislation are the Securely Protect Yourself Against Cyber Trespass Act (Spy Act) of 2005 and the Internet Spyware Prevention Act (I-SPY) of 2005.

Ethical Considerations in Cybercrime

There is a possibility that users believe finding vulnerabilities is simple. Finding defects has proven to be challenging, though, as technology and software have grown more complicated over time. Reward programs for those who find bugs have emerged because of this. Black hat and white hat hackers are currently competing to find bugs, with the possibility that the latter will prevail. It is worthwhile to look into the topic of who will uncover bugs and decide if it is morally right to sell them. It's well recognized that the work required to find software vulnerabilities involves unbalanced incentives, which could have unexpected repercussions for combating cybercrime. The methods, networks, hardware, and software used by attackers and defenders in cyberspace are the same, and there is a fundamental conflict between cyberattack and cyber defense (5).

Challenges in Combating Cybercrime

National boundaries are porous, which is a challenge that cybercrime forces states to confront for the first time. Cybercrime poses a significant threat to law enforcement, according to Europol. There are various dimensions to these difficulties. Fighting cybercrime has both technological and legal obstacles. Some special difficulties that are not present in other crimes stem from the nature of the crime itself. The most problematic aspect of cybercrime is that it may be performed from anywhere in the world and against any machine on the planet. Because online is often open to everyone, criminals can more easily penetrate the network. However, it is quite difficult to apprehend the criminals if it is done from a distance. We talked about the difficulties in fighting cybercrime here –

Legal Challenges

Cyber laws are either nonexistent or inadequate, with numerous areas where the regulations are unclear. It is challenging to provide a precise and thorough definition of cybercrimes. Many times, no commendable penalty is given. Cybercrimes inherent characteristics, cybercrimes have grown dramatically, which presents a challenge to the legal system. It makes the fight more difficult. Cybercriminals are difficult to track down. These are ghosts without names. Owing to the intricacy of the offense, it might be challenging to properly understand the law and apply it in a particular circumstance. The persistent nature of cybercriminals can be attributed to the inadequacies of the investigating agencies and prosecutors with regard to technical knowledge, ability, and tools. One might demonstrate the numerous legal hurdles that law enforcement and prosecutors encounter while pursuing cybercriminals with the short-lived but devastating career. Since traditional procedural law primarily considers tangible evidence, it is not helpful in the fight against cybercrime. Thus, it is imperative that both the substantive and procedural legislation be updated. Furthermore, because cybercrime may involve several jurisdictions, it might be challenging to pinpoint the exact location of the offense and the applicable laws.

Technical Challenges

The investigation of crimes involving computers presents significant difficulties for forensic experts. Evidence extraction from computers and servers is becoming more and more difficult due to the increased usage of encryption and access control. Cybercriminals can quickly commit crimes across borders and target several victims at once. Cybercrime presents special investigative and legal issues for law enforcement and the courts; One of these is the difficulty of locating an offender who is not present at the crime scene. Digital evidence is brittle. it might be challenging to preserve. Law enforcement organizations have limited time to conduct investigations or gather evidence due to the fast flow of data. Conventional inquiries require a lot more time. For law enforcement organizations, the proliferation of wireless internet connectivity in developing nations presents both an opportunity and a challenge. Cybercriminals communicate under anonymity. Finding the source of communication is frequently a crucial step in the investigation of cybercrime. Nonetheless, It is difficult to identify offenders due to the network's scattered architecture and the availability of various Internet services, which raises concerns regarding origin.

General Challenges

Cross-border cooperation mechanisms for the investigation and prosecution of criminal acts are slow and intricate. Police are unable to accurately monitor cybercrime due to a lack of agreement on definitions. Moreover, it costs money to combat cybercrime. Because more individuals are using the internet, there are more targets and offenders when it comes to cybercrime. Law enforcement agencies face challenges due to the growing number of internet users, as automating investigation methods can be challenging. Advanced technologies are increasing the threats associated with cyberspace. New advancements in computer and internet technology create new dimensions and speeds for crimes that are more difficult to stop. An army is not needed for an efficient cyberattack; just one person is needed. However, not only in Interpol, but in all law enforcement worldwide, there is a critical lack of knowledge and experience to combat this kind of crime (6).

Ethical challenges

Since preventing cybercrime invariably requires the use of ICT, ethical behavior demands that one avoid endangering other citizens or their data and systems. Respect for human rights and the rule of law in the relevant jurisdiction is also necessary. Online privacy is becoming more and more of a problem. It is difficult for businesses to move forward in this situation without breaking any ethical rules.

Operational challenges

International collaboration is always necessary to combat cybercrime. Treaties granting mutual legal assistance may be utilized, although doing so is frequently laborious and may not yield outcomes that are sufficiently useful to organizations. Offenders frequently include foreign nations on purpose to complicate their attacks and any investigations (7).

Framework in Combating Cybercrime

To tackle cybercrime, the following framework is used -

Legislative Framework of Cybercrime in India

The Information Technology Act of 2000 governs India's cyber legislation. (“IT ACT”). The main objective of the act is to protect individuals’ personal information and private data, which is becoming more and more crucial in today’s digital world as the number of IT-enabled services rises. More broadly, private, and sensitive data that is essential to national security must also be protected. The infrastructure needed to build up a secure system and restrict access to private data is provided by the IT Act In 2001, The United Nations Commission on International Trade Law (UNCITRAL) has endorsed the Model Law on Electronic Signatures. All states were requested to incorporate the Model Law on Electronic Signatures into their respective state legislation by the general assembly’s recommendations. In accordance with the UNICITRAL Model Law, the IT Law includes provisions regarding digital signatures. As information technology has advanced, so has the number of digital crimes. Concerns about identity theft, voyeurism, hacking, and other cybercrimes and e-commerce frauds are growing globally.

Legal Framework of Cybercrime in India

The Internet is distinctive in two ways. First, a cybercriminal can operate from anywhere in the globe and is not limited to a certain place. The second distinguishing feature is that it allows users to remain anonymous, which has its own set of benefits and drawbacks. Individuals who utilise anonymity to express themselves to the world gain from it, but those who use it to perpetrate crimes suffer the consequences. As a result, these traits make it harder to apply the law and prevent crimes. Cybercrime is punishable under a variety of laws and regulations. However, the Indian Penal Code (1860) and the Information Technology Act of 2000 govern the vast majority of legislation. The Indian Penal Code (IPC) is the country's overall criminal legislation. Which defines crimes and their consequences. The Indian Penal Code (IPC) incorporates real-world restrictions and penalties, which have been interpreted and expanded by legislation to include internet criminals (8).

The increased use of technology and the internet has resulted in a lot of bad outcomes, including as cybercrime and cyberattacks, making it harder to use technology and the internet for good, according to Anwary I (9) research. One of the biggest problems Indonesia is currently facing is cybercrime.

Every nation on the planet prohibits cybercrime as a criminal offence. The consequences of cybercrime affected computer users in Indonesia. evaluates the laws and policies the Indonesian government has put in place to combat cybercrime. Indonesian cybercrime types and trends were delineated in Articles 27 through 35 of Law No. 11/2008. The types and patterns of privacy and confidentiality infractions are delineated in Act No. 11/2008. Recommendations were made to support preventive measures; the government should improve accountability and bridge the communication gap with cybercrime authorities based on the findings of the legislative framework and analysis.

Examined the international judicial system's efforts to combat cybercrime. The international legal framework tackled three components of the problem: minimising inconsistencies between national laws, creating new authorities, and fostering international cooperation. The study by Nukusheva et al. (10) found that the core documents' ability to deter cybercrime was unaffected by the legality of international measures. The international legal system is implemented spontaneously in part due to factors such as public opinion, politics, economy, and national security. The study concentrated on the need to combine categorisation systems at the international level and provide a fundamental framework for criminal law cybercrime certification. Experts in international relations were proposed as a novel means of combating cybercrime. The latter was predicated on the idea that all governments should work together to enhance the legal framework that regulates interactions, incorporate key ideas into national legislation, and reorganise the principles of information flow.

Legislative barriers to Vietnam's fight against cybercrime were studied by Van et al. (2011). Using the legal philosophy approach, the new legal frameworks in Vietnam were examined. which comprise substantive, procedural, and preventative measures for cybercrime. To study how cybercrime law is enforced, in-depth interviews with seven senior police officers were linked with each of the four cybercrime cases. The main findings demonstrated Vietnam's dedication to update its legal system to combat and eradicate cybercrime. Despite positive results, Vietnam nevertheless faces both established and novel legal challenges were fight against cybercrime. They might make it more difficult to find a compromise between combating cybercrime and upholding human rights. Moreover employing proactive and adaptable measures in Vietnam's cyberspace management can improve the effectiveness of preventing cybercrime.

According to Anwary I. (12), the proliferation of the Internet and technological improvements have made it easier for cybercriminals to violate laws and regulations. It was led to the rapid growth of cybercrime-related problems throughout Indonesia. Much work remains to be done in the fight against cybercrime, despite the abundance of studies, laws, and legal frameworks available. By examined the relevant legal framework, the study aims to assess the role of public administration in Indonesia's fight against cybercrime. As per the results, Indonesia was a comprehensive set of policies, regulations, legislative structures in place to monitor and manage cyber security breaches and combat cybercrime. Regulating cybersecurity and fighting cybercrime, however, is a poorly executed legal framework. In addition to develop the rule of law required to exercise appropriate control over cyberattacks in Indonesia, the Indonesian government was an obligation to foresee cyber threats by developing cyber-security policies that were adequate and Outline thorough methods for guarding against cyber attacks, the scope, and types of counter measures.

According to Christou G. (13), information and communications technologies—particularly the Internet—have been increasingly significant in global politics, social life, and the economy during the past 20 years. These technologies were the foundation of the modern global information society. As a result of its growth and development, the virtual, networked ecosystem was live and become more vulnerable to serious cyber attacks, cyber espionage, and cybercrime. The European Union has been refining its rules about cyber dangers in this regard during the last ten years. Significantly lowering cybercrime was identified as a top priority goal in the European Union's Cyber security Strategy (2013), which outlined various courses of action, including improved operational capacity to combat cybercrime. Highlights the operational aspects of the Joint Cybercrime Action Taskforce of the Cybercrime Centre. It shows how the informal governance model is innovative, flexible, and collaborative, and it is confined by a formal framework that is more expansive. It reflects the intricate nature of cybercrime investigations.

According to research by Harkin et al. (14) enforcement agencies have major concerns about the growing threat of cybercrime. In response to the worries and challenges faced by law enforcement officers in the field of cyberpolicing, the study offered unique, factual data on Australian cybercrime units. Together with survey data, in-depth interviews were conducted with supervisors, key investigators, and civilian employees of two specialised cybercrime units to determine the most pressing concerns as stated by the members of these units. The field of cybercrime has an employee base that reports high job satisfaction overall, but three themes stand out: (a) the workload is growing as cybercrime becomes a more significant social issue; (b) the resources of the units were not able to keep up with the demand for workloads; and (c) the skill and training levels of the units were insufficient to handle the complexity and nature of policing cybercrime. We're listening to employee comments on how to improve the situation.

Cybercrime is a major problem all around the world, and it needs serious legislative and technological responses, as pointed out by Stanciu and Tinca (15). Because it helps create value and fosters growth over time, information is an asset that needs careful handling and preservation. Data is valuable, but it is also susceptible to frequent and violent attacks from cybercrime organisations, therefore a lot of money and people have to go into preventing cybercrime. Aside from shedding light on criminal activity and hacker tactics, the writers want to start a conversation about cyber defences and how to make them better. In order to better comprehend cybercrime and offer appropriate countermeasure options, the research sought to enhance the knowledge of senior management and government officials.

Worldwide, people have been thinking about and discussing ways to deal with the issues brought on by cybercrime, like Sarwar TB (16) has done. It has been a hotly debated subject for decades since hackers are so persistent. The goal was to have a better understanding of cybercrime and its extent. Cybercrime has been the target of efforts by various legal regimes around the globe. Examining the challenges faced by both developed and developing nations in dealing with cybercrime and its consequences, the study performed a comparative examination of the issues related to cybercrime. Cybercrime has become a worldwide phenomenon in our increasingly interconnected society, and this essay examines the national and international responses to this threat. In the fight against cybercrimes, business organisations and technologists played an increasingly important role.

There is a price to the benefits of computer technology, according to Das and Nayak (17). Computers simplify many aspects of life, but they also open government and businesses up to the most heinous form of crime: "cybercrime." These things would be nearly impossible to carry out without computers. Because of the widespread availability of affordable, powerful, and user-friendly computers, an increasing number of individuals have been able to use, and, more importantly, rely on computers on a regular basis. Criminals become increasingly dependent on them as businesses, governments, and people do. To reduce cybercrimes, they must be thoroughly examined, and the implications for society as a whole must be understood. Thus, the paper provides a methodical understanding of cybercrime and its repercussions on a range of sectors, such as socioeconomic-political, consumer trust, teen, and so on, as well as an explanation of future cybercrime developments.

Research by Calderoni F. (18) on the European legal framework for cybercrime provides preliminary evidence that cybercrime poses challenges to well-established criminal justice systems. Thus, the framework of cybercrime criminal law is examined, mostly from a European perspective. Three avenues for resolution are offered by the European legal framework: lowering the inconsistencies between national laws, granting further investigation authority, and promoting international collaboration. Every solution was covered in the study and discussed. Moreover, the argument posits that the successful execution of the primary legal instruments seems independent of the enforceability of these international measures in court. In contrast, it seems that other, non-legal elements like public opinion, politics, economics, and national security encourage the unplanned adoption of the European legal framework The Lisbon Treaty and the Stockholm Program may gradually ameliorate the problem; however, benefit of EU intervention is very minimal.

OBJECTIVE OF THE STUDY

1) To understand the legal framework regarding Cybercrime.
2) To understand the challenges faced in Combating Cybercrime.
3) To analyzing the solutions for the challenges faced in Combating Cybercrime.

RESEARCH METHODOLOGY

A research technique refers to the precise phases or methods used to gather, select, process, and evaluate data on a certain topic. In this study, data from case studies, archives, and legal framework texts were analyzed using a qualitative methodology. Primary and secondary sources serve as the foundation for the data compilation process. The major sources for legislation and administrative laws are legal documents; the secondary data is found in pertinent books, articles, and journals. A research topic must be discovered, its background must be understood through a literature review, Establishing research questions and objectives, organizing a research study, selecting a sample, collecting and analyzing data, and presenting the findings in a research report are all required steps.

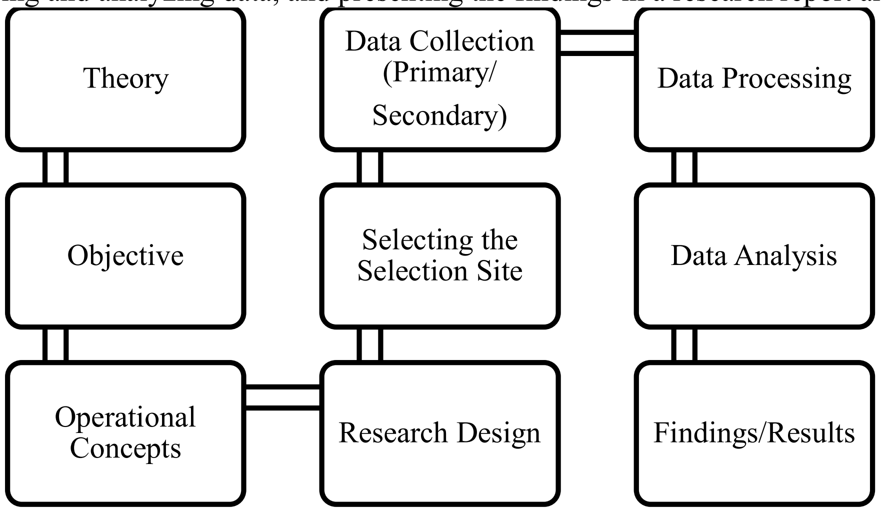

Figure 1: Research Process of the Study

RESULT

Cybercrime highlights the necessity for users of digital and cyber technologies to create laws and regulations that protect the rights of all network users. One of the most important difficulties in cybercrime is the exchange of information about cyber threats or attacks between law enforcement bodies both inside and across jurisdictions. These days, cybercrime is quite structured since the motivations behind it have shifted from individual hackers looking for attention and notoriety to professional hackers using sophisticated cybercrime models to maximize profits while evading detection.

DISCUSSION

1. To understand the legal framework regarding Cybercrime

Based on the research, India needs a special legislative framework for cybercrime because of the threats and challenges that the digital ecosystem presents. With the progress of technology and the increasing integration of the internet into our daily lives, there is an ever-increasing possibility of cyber-attacks and illicit activity. (19) Thus, to effectively combat cybercrime, complete laws and regulations must be established. Law enforcement agencies are empowered by clearly defined legislative frameworks that offer procedures, legal authorities, and rules for gathering evidence, looking into cyber events, and prosecuting offenders. (20) Because of this, India needs a special legislative framework for cybercrime to handle the changing issues brought about by the digital environment (21). The legal framework is made up of both broad rules of international law and specific regulations that have been developed to combat crime, including cybercrime. These are bilateral, regional, and multinational norms that have been established. The UN Convention against Transnational Organized Crime, popularly known as the Palermo Convention, is the primary source of international law used in the battle against crime worldwide. This groundbreaking agreement was enacted with the intention of combating organized crime—which, for the most part, includes cybercrime—more effectively (22).

There are two unique characteristics of the Internet. The first is that a cybercriminal can operate from any location in the world because it is not geographically restricted. The second unique feature is its users' ability to be anonymous, It has its own set of pros and disadvantages. It's a gift for people who utilise anonymity to convey their ideas to the public, but a bane for those who breach the law while remaining nameless. Law enforcement and crime prevention are made more challenging by these traits.

2. To understand the challenges faced in Combating Cybercrime

The international law's perspective on the difficulties in managing cybercrimes and dangers to global security. The digital age has brought about a rise in cybercrimes, which are having negative effects on both the national and worldwide levels (23). To overcome this obstacle, effective law enforcement and international cooperation are therefore required. A nation cannot resolve the problems it faces in combating cybercrime and threats to international security on its own. To address this issue, robust international cooperation and legal harmonization are required. To increase cyber security, international collaboration among governments in the information and technology sector is critical (24).

Cybercrime, often known as computer-oriented crime, is a crime involving computers and networks. The primary focus of the nation's economic and national security policies now is cybercrime. Cybercrime presents numerous issues in India. Given the increased number of cyber attacks, every company requires a security analyst to guarantee that its systems are secure. These security experts work on a variety of cybercrime-related concerns, including protecting government agencies' sensitive data and safeguarding private company servers.

3. To analyzing the solutions for the challenges faced in Combating Cybercrime

Risks will rise and services will change as the IT industry expands. Examples include online banking, e-commerce, e-government, email, social networking, and online shopping. To enable Cybercrime Forensics Investigation, a high-level solution of the total solution (CCFI) is therefore suggested. We must first ascertain the extent of the crime scene before looking into the digital devices and infrastructure that are a part of it. Next, based on the device status, we examine the static or live forensics (25). Real-Time Forensic Investigation flow is contingent upon the circumstances and cases under investigation. A typical real forensics investigation flow can be depicted in solution without any further requirements. Take a snapshot of the real and virtual memory, and then examine the network connections as they are. Second, look at the files, registry data, and details of the active execution process (26). Next, get the IP address of the currently connected network and verify its status, including the broadband device settings and current network path. Examine the system setup and user data as well as current information. Additionally, gather file and directory information, event log, and preset the process and service list (27). To effectively tackle cybercrime, develop diverse public-private partnerships with law enforcement, the IT sector, Information security organisations, internet corporations, and financial institutions (28). In contrast to the real world, cybercriminals do not vie for power or authority. Rather, they collaborate to develop their talents and even encourage one another to pursue new chances. As a result, typical law enforcement techniques are ineffective against cybercriminals (29).

When examining ways to prevent cybercrime, It is critical to consider a wide range of factors that relate to various parts of the digital world. Effective responses to the ever-evolving threat of cybercrime necessitate a confluence of technological, legal, educational, and cooperative initiatives. Establishing a robust defense against cyber threats requires cooperation and a blend of legal, technical, and pedagogical approaches.

CONCLUSION

The threat posed by cybercrime to international peace is growing. Because the criminal is always one step ahead of the law, cybercrime is always growing and becoming more sophisticated. As a result, even specialists in the legal system and the government are ill-equipped to combat it. These days, cybercrime is highly organized because the types of hackers that once sought notoriety and spotlight for themselves have evolved into professional hackers who use complex cybercrime models to maximize their profit while evading detection. As a reminder, cybercrime is extremely responsive to language, location, and regional economic trends. Because of this, these campaigns allow them to function locally, concentrating their attacks on regions and targeting particular businesses. With powerful cells dispersed over the globe that specialize in tasks that support the network, cybercrime has a loosely centralized organizational structure. Either there is no point in fighting cybercrime, or it is a global effort. The development of automation and other technology has led to an increase in cyberattacks. Governments must respond to it over an extended period. As far as fighting cybercrime is concerned, developed nations are well ahead of developing nations.

Cyber crime is a significant global issue that requires strong legislative and technical solutions. Criminal organizations with a higher economic motive are the ones coordinating the attacks. The alarming rise in criminal attacks and their financial consequences are worrying as they appear to be an upward spiral that is rupturing even the most secure networks and systems. Even though the current state of cybersecurity is not alarming, we should acknowledge that many attacks go unreported, thus it does not accurately depict the whole scope of cybercrime. Senior management and IT directors should both encourage a proactive approach aimed at enhancing information security. IT risk is now a business risk as well as a technical risk within the purview of CIOs, and it should be handled in tandem with all other major risks using an integrated strategy. Cyber criminals are not limited to a single place; Cybercrime has worldwide reach. Cyberspace is free of local geographical limits, borderless, and unregulated. Local regulations are ineffective in preventing such crimes, leaving India vulnerable. As part of its efforts to combat cybercrime, India signed a framework agreement with the United States and a cyber accord with Russia. Mr. Mode's journey to Israel to sign the Indo-Israel Cyber Framework was the country's most recent effort to streamline its cyberspace.

One of the most dangerous types of crime that occurs today is cybercrime, which occurs in a particular setting, has no boundaries, and can have very dire repercussions. It’s one of the worst kinds of organized crime, with a significant risk to society, hard times getting evidence, and hard times getting people to pay for their crimes. Due to the assumption that cybercrime accounts for a sizable portion of unreported crimes, the problem is exacerbated by the fact that very few of those who commit these crimes are now receiving sufficient punishment. The first developed nations to respond to the difficulties posed by the new wave of cybercrime were those that had been most impacted. The Convention on Cybercrime, which covers several significant topics in both substantive and procedural criminal law, was proposed and ratified on a global scale as the best legal authority in this area.

The fact that the signing governments are dedicated to promoting international cooperation, adopting appropriate measures to combat cybercrime, and harmonizing national legislation gives the Convention its unique relevance. Only when consumers become more aware of the features of cybercrime and broaden their knowledge to include ways to reduce cyber and electronic crime will cybercrime diminish. Technology improvements have provided many benefits, but they have also produced numerous drawbacks and challenges. One such problem is cybercrime, which is a sort of crime including cyber-related issues such as information security, computer security, and mobile security. Everyone finds cybercrime interesting because of the growth in information technology-related crimes.

Acknowledgements

We extend our sincere gratitude to Arunachal University of Studies, Namsai, and The WB National University of Juridical Sciences for their support and resources. Special thanks to our colleagues and peers for their invaluable feedback and encouragement. We also appreciate the assistance and cooperation of various institutions and individuals who contributed to this research. Lastly, we are grateful to our families for their continuing support and understanding during this journey.

Funding

There is no funding statement.

Conflict of interest

There is no conflict of interest.

Ethics approval

Not applicable

Data availability

Not applicable.

Abbreviation

Not applicable.

REFERENCES

1. Sviatun OV, Goncharuk OV, Roman C, Kuzmenko O, Kozych IV. Combating cybercrime: economic and legal aspects. *WSEAS Trans Bus Econ* 2021 Apr;18:751-762
2. Arifi D, Arifi B. Cybercrime: A Challenge to Law Enforcement. *SEEU Rev* 2020;15(2):42-55
3. Nuredini A. Challenges in combating the cyber crime. *Mediterr J Soc Sci* 2014;5
4. Sattar Z, Riaz S, Mian AU. Challenges of cybercrimes to implementation of legal framework. In: 2018 14th International Conference on Emerging Technologies (ICET). IEEE 2018 Nov 21:1-5
5. Oreku GS, Mtenzi FJ. Cybercrime: Concerns, challenges and opportunities. *Inf Fusion Cyber-Sec Anal* 2017:129-153
6. Sarwar TB. Analyzing the challenges of cybercrime in the global context: Need for a cross–border response. *Soc Change* 2016;10(2):37-49
7. Neethu N. Role of International Organizations in Prevention of Cyber-Crimes: An Analysis. *Nalsar Univ Law* 2020:5-17
8. Bhangla A, Tuli J. A study on cyber crime and its legal framework in India. *Int'l JL Mgmt & Human* 2021;4:493
9. Anwary I. Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach. *Int J Cyber Criminol* 2023 Jun 15;17(1):12-22
10. Nukusheva A, Zhamiyeva R, Shestak V, Rustembekova D. RETRACTED ARTICLE: Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development. *Secur J* 2022 Sep;35(3):893-912
11. Van Nguyen, Trong, Tung Vu Truong, Cuong Kien Lai. Legal challenges to combating cybercrime: An approach from Vietnam. *Crime Law Soc Change* 2022:1-22

12. Anwary I. The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia. *Int J Cyber Criminol* 2022;16(2):216-227
13. Christou G. The challenges of cybercrime governance in the European Union. *Eur Polit Soc* 2018;19(3):355-375
14. Harkin D, Whelan C, Chang L. The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Pract Res* 2018 Nov 2;19(6):519-536
15. Stanciu V, Tinca A. Exploring cybercrime–realities and challenges. *Acc Manag Inf Syst* 2017;16(4):610-632
16. Sarwar TB. Analyzing the challenges of cybercrime in the global context: Need for a cross–border response. *Soc Change* 2016;10(2):37-49
17. Das S, Nayak T. Impact of cybercrime: Issues and challenges. *Int J Eng Sci Emerg Technol* 2013;6(2):142-153
18. Calderoni F. The European legal framework on cybercrime: striving for an effective implementation. *Crime Law Soc Change* 2010;54:339-357
19. Chang LC. Legislative frameworks against cybercrime: The Budapest convention and Asia. In: The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan 2020:327-343
20. Sattar Z, Riaz S, Mian AU. Challenges of cybercrimes to implementation of legal framework. In: 2018 14th International Conference on Emerging Technologies (ICET). IEEE 2018
21. Kshetri N. Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime Law Soc Change* 2016;66:313-338
22. Nikac Z, Medic Z. Fight against cyber-crime–legislative framework and institutional mechanisms. *Emp Educ Entrep* 2020:120
23. Nouh M, Nurse JR, Webb H, Goldsmith M. Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement. *arXiv* 2019 Feb 19;arXiv:1902.06961
24. Sumadinata WS. Cybercrime and Global Security Threats: A Challenge in International Law. *Russ Law J* 2023;11(3):438-444
25. Agarwal A, Gupta M, Gupta S, Gupta SC. Systematic digital forensic investigation model. *Int J Comput Sci Sec* 2011 Jan;5(1):118-131
26. Kruse WG, Heiser JG. Computer Forensics: Incident Response Essentials. Addison Wesley 2002
27. Maung TM, Su Thwin MM. Proposed effective solution for cybercrime investigation in Myanmar. *Int J Eng Sci* 2017;6(1):1-7
28. Moore R. Cybercrime: Investigating high-technology computer crime. Routledge 2014
29. Kaur M, Kaur G, Raina CK. Cyber Crime and Its Preventive Measures. *Int J Adv Res Comput Commun Eng* 2017;6(3):920-925