# INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

VOLUME 4 AND ISSUE 1 OF 2026

INSTITUTE OF LEGAL EDUCATION

**INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY**

**APIS – 3920 – 0013 | ISSN - 2583-7990**

**(OPEN ACCESS JOURNAL)**

**Journal's Home Page – https://ijclp.iledu.in/**

**Journal's Editorial Page - https://ijclp.iledu.in/editorial-board/**

**Volume 4 and Issue 1 (Access Full Issue on - https://ijclp.iledu.in/category/volume-4-and-issue-1-of-2026/)**

**Publisher**

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

VOLUME 4 AND ISSUE I OF 2026

APIS – 3920-0012 | ISSN - 2583-7990

Published by

Institute of Legal Education

https://iledu.in

# CYBERCRIMES IN INDIA: IDENTIFYING CHALLENGES AND CRAFTING SOLUTIONS

**AUTHOR -** ANUJ WANKHADE, LL.M. (CYBER LAW) SCHOLAR, VISHWAKARMA UNIVERSITY, PUNE, INDIA

**BEST CITATION** - ANUJ WANKHADE, CYBERCRIMES IN INDIA: IDENTIFYING CHALLENGES AND CRAFTING SOLUTIONS, *INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY,* 4 (1) OF 2026, PG. 01-12, APIS – 3920-0012 | ISSN - 2583-7990.

**Abstract**

*The digital revolution in India has transformed every aspect of life, boosted the economy, and driven social development. The faster something becomes, the more dangerous it can be; thus, the growing cybercrime is a side effect of recent rapid digitalisation. Modern software attacks individual users and companies, and targets government structures as well. The most popular cybercrimes today include identity theft schemes such as phishing and ransomware attacks, as well as other forms of financial fraud and data breaches. All these expose gaps in India's cybersecurity framework. This paper takes a critical doctrinal approach to the meaning, nature, and genesis of cybercrime in India. It examines the significant current challenges that hinder the practical implementation of preventive steps and responses. The sources are primary and secondary legal sources-cum-academic works, plus policy documents that have been relied upon to provide information on existing legal frameworks for enforcement levels and on institutional capacities for our study. It also proposes different ways of changing the legal framework, and strengthening enforcement agencies, public-private collaboration, plus cybersecurity literacy. Tackling these issues is a pathway to a secure digital environment in India. This study can raise the awareness level among academicians, research scholars, enthusiasts, professionals, policymakers, as well as government officials.*

**Keywords:** Cybercrime, Phishing, Ransomware, Cybersecurity, Information Technology Act

*" I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image."*

*- STEPHEN HAWKING*

Information technology acts as a double-edged sword. When used for creative purposes, it can brilliantly enhance human potential and organisational performance.[1] However, if used for destructive purposes, it can pose serious threats not only to individuals and organisations but also to society. There has been an increase in the sophistication of computer hardware, software, and networks. People can use their computers, laptops, and smartphones in public places over free networks. This has led to new methods of committing crimes via technology, known as cybercrimes.[2]

Cybercrimes involve computer networks and fall into two categories. In the first, networks are tools for crime. In the second, criminals target networks to steal essential data, which they use for various illegal digital activities that harm organisations.[3] The term covers a broad range of targets and attack methods, from

[1] Cong Qi, "A double-edged sword? Exploring the impact of students' academic usage of mobile devices on technostress and academic performance", Behaviour & Information Technology 38, no. 12, 2019, pp.1337-1354.

[2] Hemraj Saini, Yerra Shankar Rao, and Tarini Charan Panda, "Cyber-crimes and their impacts: A review", International Journal of Engineering Research and Applications 2, no. 2, 2012, pp.202-209.

[3] Hamid Jahankhani, Ameer Al-Nemrat, and Amin Hosseinian-Far, "Cybercrime classification and characteristics", In Cybercrime and cyber terrorism investigator's handbook, Syngress, 2014, pp. 149-164.

website destruction to net banking fraud. Both public and private sector organisations find it hard to believe they could be targets of cyber-attacks. Cybercrime can affect any organisation, whether small or large.[4]

Today, digital media is used worldwide, and cybercrime has become a significant threat, transforming the criminal landscape. Cybercriminals are highly skilled in technology and use advanced methods to commit crimes. With expertise in information technology and cybersecurity, they can execute carefully planned cyberattacks to access government and corporate data, posing risks to users and governments alike.

Even amidst the growing menace of cybercrime, India has been battling with a series of challenges that include obsolete laws, inadequate cybersecurity infrastructure, paucity of trained manpower, as well as limited public awareness about safe internet practices. The experts added that the rapid technological development usually leaves a constant gap between the actual capacity of law enforcement to respond to it. This paper is thus an attempt towards filling the urgent requirement for an integrated approach against cybercrime in India through problem identification and solution orientation. It reviews and analyses the existing situation of cybercrime and what has been done so far to counter it, to strategies for raising public awareness and improving cybersecurity in India so that cybercrime rates go down.

**REVIEW OF LITERATURE**

The researcher has analysed the available and accessible literature on cybercrimes, their various types and the existing regulatory framework for them. The researcher has also referred to material on practical solutions in India. The following are some of the significant literatures which are reviewed by the author while conducting the present research:

The article "Emergence of Cyber Crime in India: Concepts & Anticipated Counter Response by Enforcement Agencies",[5] written by Sharat Kavira and Dr Amandeep Singh Kapoor, describes the increasing wave of cybercrime in India through very easy means because proper verification regarding the purchase of SIM is not done, untraceable bank accounts are readily available, and there happens to be no single coordination among all the law enforcement agencies. It therefore calls for more enhanced robust data sharing from all financial institutions, monitoring digital transactions closely, and working collaboratively with tech companies in fraud cases. This has been responded to by setting up the Indian Cyber Crime Coordination Centre. Finally, it calls for comprehensive policy interventions accompanied by proactive measures that can effectively address the burgeoning menace of cybercrime.

In the article "Cyber Crimes-Challenges & Solutions",[6] written by Rajarshi Rai Choudhury, Somnath Basak, and Digvijay Guha, explain that how cybercrime develops and becomes more complex over time in the digital world. begin by defining computer crime and discussing various types that have previously occurred, as well as new forms likely to emerge going forward. state that major problems are about: it is so difficult to detect and measure, systems are vulnerable, and there has been such rapid technological development facilitating this type of crime. This article, therefore, tries to bring out some of these forms of cybercrime, including cyber fraud and cyber terrorism, against difficulties in their detection and prosecution due to issues relating to jurisdiction, together with fast technological change. It requires close cooperation between law enforcement and the IT industry, together with the financial sector, in addressing such risks to mitigate them.

[4] *Ibid.*

[5] Sharat Kavira and Dr Amandeep Singh Kapoor, "Emergence of Cyber Crime in India: Concepts & Anticipated Counter Response by Enforcement Agencies", The Indian Police, pp.139-156.

[6] Rajarshi Rai Choudhury, Somnath Basak, and Digvijay Guha, "Cyber Crimes-Challenges & Solutions", International Journal of Computer Science and Information Technologies 4, no. 5, 2013, pp.729-732.

In the article "Emerging Challenges of Cyber Crimes to Cyber Security",[7] written by M. Tariq Banday, showcases the changing face of cyber threats and how they affect world safety. It points out the fast growth in tech and the rising smarts of cyber criminals, showing how cybercrime has moved from being a small local matter to a big global security issue. Also, this piece brings to light the high need for data safety and keeping info private because so many people use the Net, which makes them more open to cyber risks. The writer also stresses the need for global teamwork to fight the cross-border nature of cybercrime, pushing for one shared plan in cybersecurity.

In the article "Cybercrime in India: Trends and Challenges",[8] written by Juneed Iqbal and Bilal Maqbool Beigh, speaks to the growing incidence of cybercrime in India, even as internet usage sees a boom, and technology keeps getting better by the day. The authors lambast India's existing legal framework for dealing with cybercrime, pointing out inadequacies in mutual legal assistance processes between states that require streamlining, wherever gaps exist. Further typifies how vulnerable individuals and societies have become because of the massive use of smartphones and social media in an age where information is stored remotely on clouds, thus making them more accessible to cyber threats.

The article "Emerging Trends in Cyber Crimes and the Solutions",[9] written by Annapurna Jonnalagadda, M. V. J. Sastry, M. Varaprasada Rao, and V. V. Krishna, draws attention to the growing menace of cybercrimes, especially against the banking and e-commerce industries, whose bulk transactions are done online. It describes financial gain as the main motivating factor for cybercriminals who use diverse tactics, including phishing and data manipulation. It also recommends customer education, cybercrime insurance, and a partnership between law enforcement and IT in security, as well as awareness creation. The authors equally emphasise an urgent need for a formidable strategy that would ensure adequate protection against cybercrimes for businesses and consumers.

In the article "Overview about Cybercrime in India",[10] written by Priyadarsini PG and K. Poorna, highlights the rise of cybercrime and the laws. It basically speaks about the Information Technology Act, 2000, which was amended in 2008 to cover such a wide areas. Some of the miscellaneous subject matters that this article throws light upon include email spoofing and identity theft under cybercrimes. These are serious crimes against a person or an organisation where sensitive information is hacked; therefore, protection by way of following certain steps regarding cybersecurity has to be put into action, and regular monitoring of Bank Statements, Strong Passwords with a two-step method and security software for online threats are some among them which have been highly recommended by the authors too.

## RESEARCH METHODOLOGY

The present research explores the concept of crime, cybercrime, its various types, existing challenges and practical solutions. This project was prepared using the doctrinal research methodology. The researcher aims to complete the project using the doctrinal research methodology to receive the desired results. The data has been collected from different primary and secondary sources, using the library and online websites for official documents, reports, articles, journals, and books.

[7] M. Tariq Banday, "Emerging Challenges of Cyber Crimes to Cyber Security", In International Conference on Recent Advances in Electronics and Computer Engineering, India: Eternal University, Himachal Pradesh, 2011.
[8] Juneed Iqbal and Bilal Maqbool Beigh, "Cybercrime in India: Trends and challenges," International Journal of Innovations & Advancement in Computer Science 6, no. 12, 2017, pp.187-196.
[9] Annapurna Jonnalagadda, M. V. J. Sastry, M. Varaprasada Rao, and V. V. Krishna, "Emerging Trends in Cyber Crimes and The Solutions", International Journal of Multidisciplinary Advanced Research Trends 4, no. 4, 2015, p.2.
[10] Priyadarsini PG, and K. Poorna, "Overview about Cybercrime in India", Journal of Emerging Technologies and Innovative Research 11, Issue 6, 2024, pp.346-353.

Though the universe of doctrinal research is limited to the knowledge of the concept and elements of cybercrimes and related types, the research has focused on the various challenges faced by multiple stakeholders in India in combating cybercrimes. Further, this research focuses on actionable solutions to avoid cybercrime in future.

**CYBERSPACE**

The term cyberspace was first articulated by William Gibson in his 1982 science fiction novel Neuromancer.[11] Cyberspace describes the domain within which electronic media facilitate an exchange of information over computer network systems.[12] The existence of online communication provides people the ability to convey information, interact with other people and share thoughts without considering any place or location.

Now it is used to describe anything associated with computers, information technology, the Internet and the diverse Internet culture. Thus, 'cyberspace' is the electronic medium of computer networks, where online communication takes place and individuals can interact, exchange ideas, and share information.[13]

**CYBERCRIMES: OVERVIEW**

Before understanding the concept of cybercrime, it is crucial to understand the concept of crime. Britannica Encyclopaedia states, "Crime is the intentional commission of an act usually deemed socially harmful or dangerous and specifically defined, prohibited, and punishable under criminal law."[14] The essential elements of crime are human beings, mens rea (guilty intention), actus reus (illegal act) and injury.

The maxim "Actus non factum nisi mens sit rea"[15] is a well-known principle in criminal law, which states that a person is not guilty of a crime unless they had the intention to commit it. The purpose of the acts must be understood.[16] Therefore, if someone takes and carries away another person's belongings, believing them to be their own, they are not committing theft because they lack the intent to steal. The Supreme Court also emphasised that mens rea (guilty mind) is an essential element of a criminal offence.[17]

Cybercrime is not different from traditional crime because both involve acts or omissions. It is a fast-growing crime area. Criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of crimes with no borders.

Sussman and Heuston were the first authors to define 'Cybercrime' in 1995, when both computers and the internet were new and there were no cases of cybercrime.[18] As cybercrime is studied, it has been found that there cannot be a single, all-inclusive definition of cybercrime; attempts are being made to address the broader implications of such crimes as a set of actions or behaviours.

The term 'Cybercrime' refers to the commission of crimes or offences using digital communications or Information Technology.[19] A computer or a network is typically involved in these kinds of illegal actions. In Cybercrime, the criminal no longer needs to be physically present to commit the crime.[20] The victim and the attacker may never come into actual touch, which is an unusual feature of cybercrime. To evade suspicion & prosecution, hackers often function from countries that lack or have weak cybercrime laws.

[11] https://www.britannica.com/topic/cyberspace (last visited on 25th October 2025).
[12] Sanjay Sindhu and Geetika Sood, "Right to Privacy vis a vis Cyber Space: Social Perception and Legal Protection", PaKSoM, 2023, pp.295-302.
[13] *Ibid.*
[14] https://www.britannica.com/topic/crime-law (last visited on 25th October 2025).
[15] https://www.oxfordreference.com/display/10.1093/oi/authority.20110803095349253 (last visited on 25th October 2025).
[16] Abdul Sattar Ahmed Pagarkar vs. R.H. Mendsonsa and Ors. 2003 CRILJ 3790.
[17] Nathulal vs. State of Madhya Pradesh 61 1966 AIR SC 13.
[18] Divy Shivpuri, Cyber Crime: Are the Law Outdated for this Type of Crime, IJRESM Vol.4, Issue 7, July 2021, pp.44-49.
[19] *Ibid.*
[20] https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html (last visited on 25th October 2025).

Cybercrime is the most fundamental concern for law enforcement in the twenty-first century, whether we like it or not. The cyber environment, by its very nature, is borderless, providing anonymity and concealment techniques to bad actors, as well as new tools to engage in illegal conduct.[21]

In India, no statutory definition has yet been given to the term 'cybercrimes' in any law. Even after its amendment by the Information Technology (Amendment) Act, 2008, the term 'cybercrimes' is not defined in either the Information Technology Act, 2000, or the Bhartiya Nyaya Sanhita, 2023.

## TYPES OF CYBERCRIMES

### Hacking

Hacking is unauthorised access to a computer system, computer programs, data, and network resources. Hacking means acts done with the intention and knowledge to cause wrongful loss or damage to any person using information technology, or to destroy, delete, or alter data, or to diminish the value or utility of data by alteration or deletion, or any act that injuriously affects a computer or the data.[22] Section 43(a) read with section 66 of the IT Act, 2000, applies to hacking.

### Cracking

Crackers are malicious hackers who 'crack' network security to cause intentional damage. They secretly access computer systems to steal credit or debit card numbers and spread viruses, worms, and other malware. On the other hand, hackers are typically skilled programmers with expert knowledge of computer systems. They use their abilities to break into computer systems, networks, and security, often engaging in illegal activities. Therefore, when hackers cause grievous or dangerous harm to computers, computer systems, or network security, they are crackers.[23]

### Phishing

In a phishing attack, cybercriminals impersonate trustworthy entities to obtain sensitive personal information, such as usernames, passwords, and debit card details. Phishing attacks are often carried out through emails that appear to come from social networking websites, banks, auction sites, or online payment processors.[24] The cybercriminals then use the acquired information to commit fraudulent activities, such as withdrawing funds from bank accounts or misappropriating funds through other means. This can result in significant financial losses for individuals and organisations.[25]

### Viruses

Computer program viruses are programs that spread by attaching themselves to computer files. Once they are transmitted to a computer system, they infect other files on that system and may spread to other computers connected to it. Viruses often attach themselves to existing program files so that they execute when the program is run. As a result, the malicious activity of the virus does not begin until the infected program is executed.[26] Therefore, they are primarily used by criminals to infect or damage stored data on computer systems. A person is liable when viruses are inserted into a computer or computer system without the permission of the owner to destroy, delete, or alter any information therein.[27]

[21] https://www.crimeandjustice.org.uk/publications/cjm/article/understanding-21st-century-cybercrime- 'common'-victim (last visited on 25th October 2025).
[22] https://www.ibm.com/topics/cyber-hacking (last visited on 25th October 2025).
[23] Thomas Pam Gavou, John Iliya, Ekomaru Chinyere Ihuoma, and Joseph N. Gusen, "Cyber Security Enhancement in Nigeria. A Case Study of Six States in The North Central (Middle Belt) Of Nigeria", AJHSSR Vol 8, Issue 5, 2024, pp. 95-115.
[24] https://www.cloudflare.com/en-gb/learning/access-management/phishing-attack (last visited on 25th October 2025).
[25] Agboola Olayinka Taofeek, "Development of a Novel Approach to Phishing Detection Using Machine Learning", ATBU Journal of Science, Technology, and Education 12, no. 2, 2024, pp.336-351.
[26] B. K. Verma and Shashi Bhushan, "Unveiling the Threat: Exploring the World of Computer Viruses", IJIRTM Vol. 7, Issue 1, 2023, pp. 42-52.
[27] Section 43, The Information Technology Act, 2000.

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 4 AND ISSUE I OF 2026
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

**Worms**

In comparison to viruses, the worms do not require any host computer files to attach themselves to. They make functional copies and keep replicating until they consume all available memory on the computer. In this way, these parasitic programs may cause the computer system to crash. As with viruses, they may also be transmitted via the Internet or Local Area Network (LAN).[28]

**Logic Bombs**

Logic bombs are event-dependent programs; they start functioning when triggered. This means that these programs are specifically designed to execute or trigger themselves when specific events occur.[29] 'Logic Bomb' is a kind of imputation of the program into the computer with the intention that when the leading data is entered into the system on that day, this input will cause messages to be displayed on the screen.[30] Sometimes, computer viruses can cause harm and system collapse as they can be transmitted from one computer to another, leading to misconduct or misuse.

**Trojan Horse**

The Trojan Horse program is an unauthorised program that operates from within the system. Trojan, often known as the Trojan Horse, is one such malicious program that may infect the computer. It may help hackers gain unauthorised access to the victim's computers and facilitate saving files and monitoring activity on the computers. The name "Trojan Horse" is given to such a program in reference to a Greek legend.[31]

**Cyber Pornography**

Cyber pornography refers to the uploading, downloading and transmitting of pornographic pictures and writing from porn websites and online pornographic magazines, etc., to stimulate sexual and erotic desires.[32] The IT Act also prohibits cyber pornography, but only possession is not a crime under the Act.[33]

**Data Diddling**

Data diddling is a type of fraud in which raw data is altered before a computer system processes it, then restored to its original state after processing. The New Delhi Municipal

Corporation Electricity Billing Fraud Case is an example of a data diddling attack.[34]

**Email Bombing**

Email bombing involves sending a large number of emails to potential victims, which can cause an account or server to crash. It can target individuals, service providers, or companies. Email spamming is a type of email bombing. Spam can have various effects, such as blocking genuine messages from reaching ISPs by sending them thousands of unwanted messages, disrupting entire networks by consuming disk space and bandwidth, and exposing users to fraud.[35]

**Email Spoofing**

Email spoofing is a type of cybercrime in which an email appears to have been sent from one source but is actually from another. This deceptive practice can be used to harm someone's reputation or for financial gain. A spoofed email gives the false impression that it originated from a legitimate email address when it did not. This involves copying the name, logos, and graphics of a genuine organisation and creating a replica of their website.[36]

[28] *Ibid.*
[29] https://us.norton.com/blog/malware/logic-bomb (last visited on 25th October 2025).
[30] R v Thompson 1984 3 All ER 565
[31] Ashraful Goni, Md Umor Faruk Jahangir, and Rajarshi Roy Chowdhury, "A Study on Cybersecurity: Analysing Current Threats, Navigating Complexities, and Implementing Prevention Strategies," International Journal of Research and Scientific Innovation 10, no. 12, 2024, pp. 507-522.
[32] Razit Sharma and Miss Bhavika Sinha, "Cyber Pornography in India- A Legal Insight", JETIR Vol. 5, Issue 5, 2018, pp. 203-211.
[33] Section 67, The Information Technology Act, 2000.
[34] J. Star, M.L., "Nuances on Cybercrime with special reference to Data Diddling - A study", JETIR Vol. 10, Issue 10, 2023, pp. 315-316.
[35] Babita Rani Srivastava, "Cyber-crime: a threat to national security", Journal of Social Review and Development 3, Special no. 1, 2024, pp. 80-83.
[36] https://us.norton.com/blog/online-scams/email-spoofing (last visited on 25th October 2025).

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 4 AND ISSUE I OF 2026
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

### Cyber Stalking

Harassing behaviours are most often defined as stalking. It can take on many

forms that may include following the individual, repeated harassing phone calls, leaving threatening messages and sending unwanted items. Stalking does develop into more serious acts of violence -for example, inflicting physical harm on the victim. The pattern of behaviours by the individual doing the stalking defines it. Thus, any use of online services to perpetrate continuous harassment against a victim amounts to cyberstalking.[37]

## JURISDICTION IN CYBERCRIME

Cyberspace does not have physical boundaries. It is a space that keeps growing, and with just a click of a mouse, one can access any website from anywhere in the world. Since the websites operate under terms of service agreements, privacy policies and disclaimers, subject to their own domestic laws, transactions with any of the websites would bind the user to such contracts.[38]

The IT Act, 2000 provides that this Act shall also apply to any offence or contravention committed outside India by any person of any nationality."[39] It further applies to an offence or contravention committed outside India if the act or conduct constituting the offence involves a computer, computer system, or computer network that is located in India.[40]

It is the legislative function of the Government to make laws and the judicial or administrative function to carry out those laws. Therefore, whatever principles of jurisdiction a State applies, it must not go beyond the limits that international law imposes upon its authority.

## CHALLENGES IN COMBATING CYBERCRIMES

As technology grows, the internet gets inside daily life, which means that over time, cybercrime becomes more prevalent, wherein a lot of crimes over the web are committed against somebody or something. First of all, it has to be noted that fighting cybercrime is a matter of quite complicated and multidimensional challenges due to the virtual space in which this type of crime takes place.

### Jurisdictional Challenges

Cybercrimes may be instituted from anywhere, making it very hard to know which particular jurisdiction's laws are applicable. Online crimes may take place affecting victims in more than one country; hence, the complexity of legal responses and enforcement efforts increases. Challenges are also presented to the courts in asserting jurisdiction over cross-border cybercrime. While often relied upon, the principles of territoriality, nationality, passive personality, universality, and protective principal application can be inconsistent, hence difficulties in prosecution.[41]

This problem may involve countries with different legislations on search and seizure. It may impede the efforts of law enforcement agencies to garner all the required evidence across borders. The seamless perpetration of cybercrime across borders calls for robust international collaboration among law enforcement agencies. However, varying legal standards and procedures introduce barriers to cooperation and, hence, the coordination of investigation and prosecution.

### Lack of a Uniform Legal Framework

Cybercrime carries different meanings across countries, thereby leading to confusing and inconsistent legal interpretation. It means that in some places where certain acts are considered offences, they are not controlled by law in others; hence, a treaty cannot compel those states to act against specific activities.

[37] https://fire.kerala.gov.in/wp-content/uploads/2022/08/journal-vol10.pdf (last visited on 25th October 2025).
[38] *Ibid.*
[39] Section 75 (1), The Information Technology Act 2000.
[40] Section 75 (2), The Information Technology Act 2000.
[41] https://www.scconline.com/blog/post/2024/03/24/jurisdiction-in-cybercrimes-and-civil-disputes (last visited on 25th October 2025).

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 4 AND ISSUE I OF 2026
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

There is no unified standardised legislation, which means that one country's laws about obtaining evidence, privacy of data, and how to charge cybercriminals may differ from those of another. The disparities can actually make it very hard for enforcement bodies to work together due to conflicting legal requirements.[42]

Also, the absence of solid international legal standards points to the fact that global standards are needed to address cybercrime. Efforts such as the Budapest Convention on Cybercrime merely strive to make a somewhat more harmonised approach but getting most countries on board and actually in practice is a major hurdle.

**Technical Challenges**

Technological innovation moves at a rapid pace; thus, new tools and platforms are constantly changing. Typically, cybercriminals use the most recent technologies to perpetrate their crimes. This makes it very challenging for law enforcement to be on an equal footing with the same methods and tools being applied in cyber offences. Also, the great amount of data created and stored in digital environments gives a big headache to investigators. Large datasets require analysis to sift pertinent evidence; this can be both time-consuming and resource-intensive, with delays that bog down the investigation process even more.[43] Most of these cyber criminals are applying encryption as well as anonymising technology-imposing VPNs, plus the dark web, their identity and actions remain hidden; thus, law enforcement finds trace back routes to criminal activities arduous while obtaining actionable intelligence.[44]

**Evidence Collection and Preservation**

Data on devices can be altered or deleted, and network logs can be overwritten. Digital evidence is also very delicate and can be easily changed or overwritten.[45] This means that it is crucial to act quickly to secure evidence, which can be challenging in fast-moving cybercrime situations. Collecting and analysing digital evidence requires specialised knowledge and skills in digital forensics, and investigators need to be trained to handle different types of digital media, such as hard drives, cloud storage, and mobile devices, each of which may require different techniques for evidence extraction.[46]

The acquisition of digital evidence often raises issues of legality and privacy. Here again, the investigators have to manoeuvre through the intricate provisions relating to data privacy and surveillance, varying from one jurisdiction to another. While one has to respect individuals' rights, balancing with the evidence required does make the investigation more complicated.[47]

**Anonymity and Encryption**

The internet provides several ways for people to stay anonymous, such as using Virtual Private Networks (VPNs) and other technologies that anonymise their online activity. This anonymity makes it challenging for law enforcement to trace illegal activities back to the individuals responsible, as cybercriminals can hide their identities and locations.[48] The dark web can also be used to do it, which is a part of the internet that is not searchable through regular search engines and requires specific software to access. It is used for illegal activities, including drug trafficking, weapons

[42] UNODC Comprehensive Study on Cybercrime Draft, February 2013 (available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf).

[43] David S. Wall, Cybercrime: The transformation of crime in the information age, John Wiley & Sons, 2024.

[44] *Ibid.*

[45] https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/forensic_science/16._digital_forensics/33._digital_crime_scene_investigation/et/6317_et_6317_et_et.pdf (last visited on 25th October 2025).

[46] Gagandeep Kaur and Anshika Dhawan, LAWS OF ELECTRONIC EVIDENCE AND DIGITAL FORENSICS, PHI Learning Pvt. Ltd., 2024.

[47] *Ibid.*

[48] Marjolaine Biscop and David Décary-Hétu, "Anonymity technologies in investigative journalism: a tool for inspiring trust in sources", Journalism Practice 18, no. 6, 2024, pp.1420-1441.

sales, and the distribution of stolen data.[49] The anonymity. This is the major reason why it becomes very difficult to trace and nab perpetrators active in this domain. Further, cybercriminals usually make use of strong encryption to communicate their codes and data.[50] While encryption is necessary for privacy and security purposes, it may make it difficult to access crucial evidence by law enforcement.

**Resource Limitations**

Many law enforcement agencies operate under tight budgets, which can limit their ability to invest in the technology, tools, and training needed for cybercrime investigations. Limited financial resources can lead to outdated equipment and inadequate software, making it challenging to keep pace with evolving cyber threats. There is often a shortage of personnel with the specialised skills and knowledge required to investigate cybercrimes effectively.[51] Cyber Forensic teams usually require modern equipment that may not be readily available within many law enforcement agencies. As a result, this slows down the investigations and reduces the overall effectiveness of cybercrime units.[52]

By overcoming all odds, law enforcement personnel must continue training to stay up to date on the latest cybercrime trends, technologies, and investigative techniques. However, resource limitations can restrict access to training programs, workshops, and conferences, leaving personnel ill-equipped to handle complex cybercrime cases.[53]

**International Cooperation**

Political discrepancies between countries can stand in the way of investigating cybercrimes that were committed against a particular country. Diplomatic relationships also play a very important role; many countries are not ready to cooperate, share information, and assist in investigations due to diplomatic ties.[54] Building trust among all international partners is fundamental in practical cooperation. The lack of confidence that their data is safe and secure and will not be used against them later, however, most countries become reluctant to fully cooperate.[55]

The legal processes of international cooperation can be rather slow and arduous. In most cases, it takes a long time to process requests for mutual legal assistance, thereby delaying the investigation and giving room for cybercriminals to escape.[56]

**Public Awareness and Education**

Most people and organisations do not understand the risk factors that pertain to cybercrime. Phishing, malware, and identity theft attacks are examples of prevalent attacks due to a lack of knowledge.[57] There is a general misapprehension about what constitutes and how extensive cyber threats are. Most individuals think that cybercrime is something remote from their immediate concerns; hence, they do not implement precautionary measures. This misplaced perception underrates the need for urgency in adopting cybersecurity practices. Raising and maintaining interest in such learning and awareness programs for cybersecurity is still a challenge because most people do not perceive an immediate connection with their daily undertakings.[58]

[49] https://www.experian.com/blogs/ask-experian/what-is-the-dark-web (last visited on 25th October 2025).
[50] *Ibid.*
[51] Allison Peters & Amy Jordan, Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime, JNSLP Vol. 10, 2020, pp. 486-524.
[52] Nikhil Bajpai and Munish Swaroop, "Unravelling E-Evidence: The Role of Cyber Forensics in Digital Investigations", Indian Journal of Law and Legal Research 6, no. 1, 2024, pp.1873-1891.
[53] *Ibid.*
[54] Hengyue Zhang and Xiangqian Gong, "The research on an electronic evidence forensic system for cross-border cybercrime", The International Journal of Evidence & Proof 28, no. 1, 2024, pp.21-44.
[55] *Ibid.*
[56] Anna-Maria Osula, "Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data", Masaryk University Journal of Law and Technology, Vol 9, Issue 1, 2015, pp.43-64.
[57] https://cybercrime.gov.in/pdf/Cyber%20Security%20Awareness%20Booklet%20for%20Citizens.pdf (last visited on 25th October 2025).
[58] *Ibid.*

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 4 AND ISSUE I OF 2026
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

## SOLUTIONS FOR CYBERCRIMES

A multifaceted approach is required for the enhancement of legal frameworks, improvement of international cooperation, and raising public awareness. Clear laws and friendly collaboration between different jurisdictions and an aware public on matters concerning cyber threats are what can firmly lay down resilient defence systems against the mounting threats of cybercrime to safeguard our digital future.

### Strengthening Legal Frameworks

Countries may look at a proposal through international treaties identical to the Convention on Cybercrime of the Council of Europe, signed in Budapest. That particular treaty provides a framework within which global cooperation and harmonisation of laws can be developed to ensure consistent and effective responses to cybercrimes.[59] It initiates by developing model laws that different jurisdictions can implement so as to standardise the definitions and penalties, hence facilitating cross-border law enforcement. Regular reviewing and updating of legal frameworks are also essential to ensure they keep pace with the level of technological advancements and new tactics used in cyber threats, through new forms of cybercrimes. It should also consider the impacts brought about by emerging technologies like artificial intelligence and blockchain technology on legislation, specifically relating to their potential misuse for cybercrime.

### Enhancing Law Enforcement Capabilities

Specialised training of the law enforcement officers on cybercrime investigation, digital forensics, and legal aspects of cyberspace would give pertinent skills to effectively tackle the menace.[60] Another program proposed is continuous training programs for law enforcement on emerging cyber threats, new technologies, and updated investigative techniques. To facilitate this, agencies should support the acquisition of the most advanced digital forensic tools in analysing electronic evidence, conducting data recovery, and tracing activities related to cybercriminals.[61] It should also sensitise the community and private sector about cyber threats and encourage them to report any suspicious activity.

### Promoting International Cooperation

An international treaty should be developed, setting unified standards of cybercrime legislation, application, and mutual legal assistance. Treaties like these open the way for cross-border investigation and prosecution. The creation of joint databases on cyber threats, trends, and offenders would raise attention levels and improve response strategies.[62] Secure information exchange channels between law enforcement and intelligence agencies to respond jointly with other interventions would make interventions more effective.[63] Active participation in global cybersecurity plus cybercrime forums enhances dialogue plus cooperation, besides best practices as well as new threats.

### Public Awareness and Education

Workshops and seminars for such groups as students, parents, and seniors will give practical tips on safe digital navigation. Other means are the use of traditional and social media to sensitise the public.[64] It entails a great campaign in which the major cyber threats awareness is carried out-sharing information about identity theft, ransomware, and online scams, but with prevention tips that are immediately actionable. Local community

[59] Olukunle Oladipupo Amoo, Akoh Atadoga, Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Femi Osasona, and Benjamin Samson Ayinla, "The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system", World Journal of Advanced Research and Reviews 21, no. 2, 2024, pp. 205-217.

[60] S. Sharma, "Digital Forensics: Legal Standards and Practices in Cybercrime Investigation," 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), Noida, India, 2024, pp. 1-6.

[61] *Ibid.*

[62] Aparna Chandra and Shova Devi, "The Need for International Co-Operation in Combating Cyber Crime", MSB-IJIR Vol. 2, Issue 3, 2024, pp. 504-512.

[63] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf (last visited on 25th October 2025).

[64] L. Meghan Mahoney and Tang Tang, Strategic social media: From marketing to social change, John Wiley & Sons, 2024.

involvement through events, talks, and demonstrations helps build the culture of cybersecurity awareness.[65] Moreover, partnering with community organisations boosts the outreach too and special attention should be given to vulnerable elderly people and children who are more prone to cyber threats.

**Implementing Technical Solutions**

Firewalls ensure packet inspection and access control between the trusted internal networks and untrusted external networks, in line with rules.[66] Sensitive data at rest and in motion should be encrypted to avoid unauthorised access; encryption makes sure that the data is not readable without the right decryption keys. This is key when personal or financial information is concerned.[67] The use of secure protocols like HTTPS, SSL/TLS, and VPNs ensures the protection of data being transmitted over the internet from being intercepted by cybercriminals.[68] Software, operating systems, and applications should also be kept up-to-date because known vulnerabilities are regularly patched through updates that can otherwise be exploited by hackers.

**Encouraging Private Sector Collaboration**

Governments may develop schemes for public-private partnerships that would encourage the sharing of information and cooperation in fighting cyber threats. This would improve the abilities of both sectors to address the issue of cybercrime.[69] In addition, threat intelligence sharing platforms keep organisations informed about emerging threats and vulnerabilities with information on attack patterns, malware signatures, and incident reports.[70] Organisations can practice response strategies through joint simulations of a cyber incident, hence improving coordination between the public and private sectors.

**Utilising Technology and Innovation**

Artificial Intelligence and Machine Learning based algorithms can be leveraged to detect any pattern or anomaly within huge volumes of data that may be associated with cyber threats. Therefore, business organisations shall leverage these cutting-edge technologies for speedy as well as highly accurate threat detection so that a probable incident can be pre-empted effectively.[71] Blockchain offers a very secure and tamper-proof way of storing as well as sharing information.[72] This is essentially important in sectors such as finance or healthcare, where the integrity of information is crucial. Cloud service providers normally implement very advanced security measures, including encryption and multi-factor authentication, to ensure the safety of information.

**Fostering a Cybersecurity Culture**

Clear communication about any suspicion of any activity or a potential

security incident will help employees to speak out about their concerns, hence establishing clear communication for reporting any suspicious activity.[73] Once employees are given an avenue to provide feedback on the cybersecurity practice, they own and internalise the practice as their own security effort of the organisation. Security should be integrated into consideration in all the daily activities and decisions made by employees; therefore, this paper aims to assist the organisation in

[65] *Ibid.*
[66] https://www.kaspersky.com/resource-center/definitions/firewall (last visited on 25th October 2025).
[67] https://cloud.google.com/learn/what-is-encryption (last visited on 25th October 2025).
[68] Rupam Hazra, Parag Chatterjee, Yash Singh, Gopal Podder, and Titli Das, "Data Encryption and Secure Communication Protocols", In Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning, IGI Global, 2024, pp. 546-570.
[69] https://www.unodc.org/documents/NGO/PDF/CSU-CyberCrime-240807-WEB.pdf (last visited on 25th October 2025).
[70] *Ibid.*
[71] Yijie Weng and Jianhao Wu, "Leveraging Artificial Intelligence to Enhance Data Security and Combat Cyber Attacks", Journal of Artificial Intelligence General Science (JAIGS), no. 1, 2024, pp. 392-399.
[72] Yazeed Yasin Ghadi, Tehseen Mazhar, Tariq Shahzad, Muhammad Amir khan, Alaa Abd-Alrazaq, Arfan Ahmed, and Habib Hamam, "The role of blockchain to secure internet of medical things", Scientific Reports 14, no. 1, 2024, 18422.
[73] Öykü Işik, Yanya Viskovich, and Si Pavitt, "Common pitfalls when mitigating cyber risk: Addressing socio-behavioural factors", Cyber Security: A Peer-Reviewed Journal 8, no. 1, 2024, pp.6-23.

inculcating a security-first mindset.[74] This should further motivate and attract attention through recognition of employees who have good cyber hygiene; hence, it is supposed to focus on continuous learning, so that new threats can keep the organisation resilient.[75]

**CONCLUSION**

The challenges of cybercrime in India require immediate, strategic responses. With increasing digital space, complexities and massive frequencies of cybercrimes are imposed on the safety of individuals, corporate bodies, and even the nation itself. Major challenges recorded in this study include inadequate extant legal frameworks to address such issues appropriately, insufficient training of law enforcement on the provisions therein, and public awareness about cybersecurity.

India has to prioritise the development of an appropriate, comprehensive legal framework in response to the rapidly changing nature of technology and cyber threats. It involves not only amending the Information Technology Act but also enacting new laws on emerging forms of cybercrimes. The other aspect is international cooperation, since most hackers operate from outside the country's borders. Joining hands with international policing bodies and signing treaties will enhance investigation capacities, besides facilitating information exchange. Public awareness is also instrumental through campaigns informing people of internet nuisances and advocating safe digital usage.

In summary, building up a resilient cybersecurity environment in India requires an initiative involving government and law enforcement, together with the private sector and civil society. Addressing the challenges identified above and taking practical steps toward their solution will go a long way in fighting cybercrime against the Indian population as well as ensuring a safe digital ecosystem that promotes economic growth through innovation.

**SUGGESTIONS**

The researcher wants to suggest the following points:

- There should be the development of specialised training programs for law enforcement agencies to improve their skills in cybercrime investigation and digital forensics.
- Launching nationwide campaigns to educate citizens about cyber risks and safe online practices, integrating cybersecurity education into school curricula.
- Engagement in partnerships with other countries to share information and best practices will help to combat transnational cybercrime.
- There should be an allocation of resources for advanced technological tools and infrastructure that aid in the detection and prevention of cyber offences.
- There should be user-friendly platforms for citizens to report cybercrimes, ensuring accessibility and anonymity to encourage reporting and promote it at the grassroots level.
- Promoting cybersecurity research initiatives to develop innovative solutions and support will help grow cybersecurity startups.

[74] *Ibid.*
[75] https://oertx.highered.texas.gov/courseware/lesson/4779/student/?section=8 (last visited on 25th October 2025).