International Journal of Social Science Research (IJSSR)
Volume- 3, Issue- 1 | January - February 2026 ISSN: 3048-9490

Cyber Crimes in India: Challenges and Legal Reform

Afzal[1*] & Anurag Singh[2]
[1,2] Faculty of Law, University of Lucknow

Abstract

In the age of digital advancement India's e-governance, e-businesses, and social activities continue to become more digitalized and with this digitalization new and emerging forms of cybercrime also have evolved which attacks on the personal computer system and breaches the data of the individual. The use of the Internet and e-commerce has increased rapidly around the globe. A large number of nations, particularly those categorized as developing nations, are making significant investments in the creation and improvement of IT infrastructure, guaranteeing a strong telecommunications infrastructure, and promoting the use of the Internet and cyberspace in business, government, and various communities. The widespread usage of ICTs has caused cyber activities to grow quickly all across the world. Information and communication technology have revolutionized businesses, generated economic prosperity, and ensured contact between countries throughout the globe. This article explores how India tackles cybercrime. It covers the main laws like the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023 that shape the country's view regarding the protection of the personal data. India's set up these rules to keep people safe online. The article also looks at what institutions are doing to help such as the National Cyber Crime Reporting Portal. This portal is a place where people can report cybercrime. The government is also helping by setting up labs to investigate cybercrime, at both the central and state levels. These labs are called forensic infrastructure and they help the government understand and examine the digital evidences to solve cybercrime cases easily.

Keywords: cybercrime, data protection, identity theft, artificial intelligence, deep fake

"As the world is increasingly interconnected, everyone shares the Responsibility of securing cyberspace."

- Newton Lee

Introduction:

Cybercrimes are seen as a major challenge in this age because of the rapid evolution of information and communication technologies and their use in various aspects of our lives and our growing reliance on these technologies for our economic, social, and governmental activities. Various aspects of cybercrimes include hacking, identity thefts, cyber frauds, cyber

[*]Corresponding Author Email: afzalkhan120592@gmail.com
Published: 10 February 2026
DOI: https://doi.org/10.70558/IJSSR.2026.v3.i1.30820

stalking, cyber breaches, cyber terrorism, and many others based on our vulnerabilities or weaknesses as human beings and our vulnerabilities with regard to technological evolution. The emergence and development of e-commerce and electronic payment systems have increased our exposure to cybercrimes risk as never before through our increased involvement with cybercrimes. This threat of cybercrimes risks is seen not only as a threat to individuals and organizations but also to States and countries at large. Unlike any other crimes, cybercrimes are multinational crimes with regard to their anonymity and technological involvement, and this brings about a major challenge with regard to their investigation and persecution. The risk of cybercrimes is not seen as only a risk relating to economic activities but also as relating to national security and confidentiality and our faith and trust.

India's rapid development to utilize digital technologies in recent years has been driven by various factors such as Digital India initiatives[1], affordability of Internet service, increased use of smartphones, and growth of various forms of digital payment systems. The growth of e-governance systems in India has also spurred increased use of various forms of e-governance systems in recent years. The increased use of e-governance systems has also complemented increased growth in e-banking systems in India in recent years. The increased use of various forms of e-governance has spurred growth in e-commerce systems in India in recent years. The growth of various forms of e-governance systems has also increased in recent years due to increased use of telemedicine systems in India in recent years.

Classification of Cyber Crimes:

The term cybercrime means the criminal acts perpetrated through the use of digital technologies. It can either be through targeting computer systems or making use of computer systems in the process of crime. It encompasses a broad area that keeps widening due to the use of information technology. All cybercrimes can be divided mainly into two parts, i.e., when a crime is committed targeting a computer, as well as when a crime is facilitated through a computer. The first part comprises hacking, virus conduits, and denials of services, while the second part comprises internet scams, cyber stalking, and dissemination of illicit materials, amongst others. Not only affecting an individual incident of cybercrime affects corporate entities, infrastructures, as well as between governments. It should be noted that while gain remains the major reason, cybercrime can also be motivated by other causes like ideologies, politics, or pure malevolence.

Cybercrimes are broadly classified on the basis of purpose and its intent. Fundamental classification and distinction between crimes against persons, crimes against properties and crimes against states as follows;

Crimes against Persons**:** Those are committed against a person, psychological damage, and

[1]"Digital India is owned company by experts who have been in the e-gov services industry since 2017. The company establishes business relationships with operators, consumers, merchants and vendors networks, financial institutions and infrastructure providers. Digital India plays a critical role ensuring the success of the system, allowing to all parties to maximize the benefits"< https://www.digitalindiaportal.co.in/about.php> accessed 13 January 2026

damage to reputation. Key examples are cyber stalking[2], harassment, identity theft[3]-that is, using personal information for fraud-and the malicious creation of deep fakes with the intention to defame or blackmail. Cybercrimes against persons also includes the child pornography.

Financial Crimes: This is one of the most common classes, targeting economic theft directly. It ranges from online fraud-that is phishing and investment scams-to ransomware that is, extorting money by encrypting data to unauthorized financial transactions. Crime related copyright also come into this category.

Crimes against state: These threaten national security and public order. Cyber terrorism[4] consists of such an attack on important infrastructures like power grids, banking to instill fear. Cyber war and espionage fall into this category, together with using digital platforms to spread major disinformation.

Other Classifications: Crimes can also be categorized based on the means of the attacker, where the means can include hacking, malware distribution, or denial of service attacks that serve any of the above intentions. This would provide a structured categorization that will, in turn, help formulate specific legal frameworks and specialized cyber security responses.

Emerging Trends of Cyber Crimes in India:

The digital revolution that has swept across India, thanks to the widespread adoption of the internet and the subsequent digitalization of the country, has been a boon for the economy and society. However, this revolution has also created an ideal breeding ground for cybercrimes, which are crimes that use technology as a means to commit fraud, steal data, or disrupt systems. In recent years, the incidence of cybercrimes in India has escalated to an alarming rate, from simple phishing and malware attacks to highly sophisticated ones.

One of the most important trends in the Indian cybercrime scenario is the rapid rise in the number of cyber frauds and financial crimes. According to recent statistics, there have been millions of complaints of cybercrime in India in 2023-2024, with the number of complaints increasing sharply every year. Between 2021 and 2024, the number of complaints to the National Cybercrime Reporting Portal (NCRP) has increased from around 1.37 lakh to over 17 lakh, mostly because of digital frauds and online financial crimes. The total estimated loss due to cyber fraud in 2024 was over ₹22,800 crore.

“The National Cyber Reporting Platform (NCRP) of the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs is a centralized online platform for registering cybercrime complaints, which are automatically assigned to the relevant States or

[2]The Bhartiya Nayay Sanhita, 2023 § 78

[3]The Information and Technology Act, 2000 § 66C: Punishment for identity theft. Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

[4] ICT Cyber Desk, ‘Cyber Crime and Cyber-Terrorism, January-March 2016’ (International Institute for Counter -Terrorism (ICT) 2016) <https://www.jstor.org/stable/resrep09466.6>accessed 22 January 2026.

Union Territories (UTs). It is clarified that neither NCRP nor I4C has the authority to place liens, freeze, or unfreeze bank accounts. The responsibility lies with the law enforcement agencies (LEAs) of the respective States/UTs, as per provisions of BNSS/CrPC. The Indian Cyber Crime Coordination Centre serves as a platform for reporting complaints and does not exercise administrative control over LEA actions within States/UTs. I4C's role is limited to coordinating with LEAs and other stakeholders for cybercrime prevention and detection efforts."[5]

One of the most common financial scams is the "digital arrest" scam, in which scammers pose as policemen or government representatives and force victims to transfer funds to avoid arrest or legal proceedings. This type of cybercrime has been particularly common among senior and technologically unsaved citizens, causing losses of thousands of crores of rupees every year in different states.

Phishing and social engineering attacks have remained common modes of operation for cyber crooks. These types of attacks involve misleading messages, emails, or websites that imitate genuine ones to deceive victims into sharing confidential information like passwords, bank account details, or authentication codes. The advanced nature of these attacks has escalated with the emergence of artificial intelligence (AI), enabling scammers to disseminate highly misleading texts and even audio or video recordings that appear as trusted figures.

AI-driven threats aren't just a tech buzzword anymore they're actually keeping people up at night. Cyber attackers are getting crafty, using machine learning to spin up fake emails, sneaky apps, and digital traps that can breeze right past old-school security. And it's not just that these attacks are happening more often. They look a lot more real, which makes life tough for everyone regular folks and cyber security teams.

Malware and ransomware like Infostealer, Lumma Stealer, and RedLine isn't just floating around its already hit tens of thousands of computers, scooping up passwords and banking info. Ransomware attacks keep going up, too. Hackers lock up computers and demand a payout to set them free. Schools, hospitals, even critical infrastructure they're all getting hit.

Lastly, the cybercriminals are targeting mobile and identity systems too. SIM swap scams, for example, and abusing Aadhaar-SIM links these tricks are popping up all over. Attackers spot weak points in telecom and identity checks and slip right through, stealing money or breaking into accounts, often without anyone catching them because sometimes it operated from the cross border.

The Indian cybercrime scene is tangled up with international operations and organized crime rings that use global networks to run scams. That makes it way harder for anyone to track them down or bring them to justice.

Prevention of Cyber Crimes and Challenges:

Cyber law has numerous territorial and jurisdictional restrictions as cybercrimes are not limited by territorial boundaries. Though the Information Technology Act, 2000 is applicable

[5] <https://cyberpolice.nic.in/> accessed 12 January 2025

to the whole of India[6], its extraterritorial operation is restricted. Section 75 is applicable only if a computer system or network in India is involved. Cybercrimes committed outside India without any clear nexus to India cannot be easily prosecuted. Tracking down where a cybercrime actually happened isn't easy. Everything's online, so borders get blurry fast. When more than one country says, "Hey, this case is ours," things get complicated fast. Getting everyone to cooperate isn't easy, but you really need countries on the same page mutual legal assistance treaties are a big deal when you're chasing criminals across borders. Still, just gathering evidence that actually works in another country's court? That's a headache because different countries have different cyber law which is applicable to its own territory.

Consider India. The National Cyber Crime Reporting Portal, CERT-In, and cybercrime cells are all available in the nation. It is difficult to accomplish anything without a strong infrastructure and a sufficient number of highly qualified cyber forensic specialists. Things just stall if you don't have the cyber expert or resources, even though the tools are available. Investigations are prolonged by agencies' poor collaboration and frequent jurisdictional disputes. Agencies don't work together well, and everyone keeps running into jurisdiction fights, which just drags out investigations. Plus, technology keeps racing a head encryption, anonymization, dark web tools, and data stored overseas are all way ahead of what the law and current systems can handle.

In India, cybercrime cases frequently get delayed because investigations drag on and convictions are rare. Is the real problem? Law enforcement teams just don't have enough cyber forensic skills or modern tech to keep up. They're working with old tools and struggling to get evidence from third parties and Foreign Service providers mostly because the process for getting international help is a mess and takes forever. Jurisdiction issues and the absence of dedicated cyber courts slow things down even more. When evidence isn't handled right and digital chains of custody break, cases fall apart. Trials take too long, conviction rates stay low, and in the end, cybercrime laws lose their bite.

In the Indian context, the prosecution of cybercrimes faces several forensic and evidence related challenges. Electronic evidence[7] is extremely volatile and can be easily destroyed or tampered with if it is not preserved in time. The investigating agencies also lack experts in cyber forensic analysis and adequate forensic facilities. It is also difficult to preserve the authenticity, integrity, and chain of custody of cyber evidence in the existing procedural laws. The lack of uniform forensic standards and the limited knowledge of the judiciary about the technical evidence further add to the challenges.

Cross border Cybercrimes

Cross-border and transnational cybercrimes happen when the people involved from abroad, the victims, the data, or even the technology itself are scattered across different countries. Cybercriminals operated the attackers that the internet doesn't care about borders it gives them plenty of places to hide. In India, the Information Technology Act of 2000 has the

[6]The Information and Technology Act, 2000 §§ 1(2), 75
[7] The Bharatiya Sakshya Adhiniyam, 2023 §§ 2(1)(d) & 2(1)(e), 57, 61, 62, 63

extraterritorial operation it means the Act has jurisdiction to try the cases outside the country in some situations, but honestly, things are complicated. Each country wants to protect its own territory, and their laws different. To tackle these criminals usually means countries have to cooperate and rely on Mutual Legal Assistance Treaties (MLAT), but that process is not easy. Getting information takes forever, countries argue over who's in charge, and international cyber laws just don't line up. All of this makes it seriously tough to catch and prosecute the cybercriminals who attacks from cross border.

Cyber Crimes in India: Legal Framework:

India's main law on cyber activities and digital crime is the Information Technology Act, 2000. This act gave legal status to things like electronic transactions and digital signatures it basically created the ground rules for e-governance and fighting cybercrime. To keep up with tech changes, it also updated big laws like the penal code and the rules of evidence.

Before this, people who committed crimes online faced charges under the old Indian Penal Code from 1860. So, if someone cheated, intimidated, or defamed another person using digital tools, the law still went after them the only difference was that the crimes happened online.

In 2023, the Bharatiya Nyaya Sanhita (BNS) replaced the IPC. The BNS is a more modern take on criminal law, and it covers cybercrimes too even if it doesn't spell out "cybercrime" in detail. Courts and legal experts agree: lots of classic crimes like fraud, theft, or harassment also apply when they're committed online.

There's also the Digital Personal Data Protection Act, 2023 (DPDP Act). This is India's first law focused just on protecting digital personal data. Parliament passed it in 2023, and it's being rolled out in steps. Right now, some of the key rules and compliance systems are already up and running.

Institutional Reform:

As India's digital world keeps expanding, cybercrimes are picking up too. Tackling these new risks takes more than just good intentions it calls for strong policies and institutions that can keep up. The Indian government has built a pretty robust setup to handle this, layering together reporting tools, technical teams, special programs, and training efforts to stay ahead of the game.

National Cyber Crime Reporting Portal (NCRP)

The National Cyber Crime Reporting Portal (NCRP) is a big step forward from the Ministry of Home Affairs[8]. It's a one-stop platform where people can report cybercrimes online think financial fraud, identity theft, cyber stalking, child sexual abuse material, or online harassment. Not only does this portal make it easier for victims to get help, but it also brings

[8] The National Cyber Reporting Platform (NCRP) of the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs is a centralized online platform for registering cybercrime complaints, which are automatically assigned to the relevant States or Union Territories (UTs). < https://cyberpolice.nic.in/> accessed 15 January 2026

law enforcement agencies together, so investigations move faster. The Indian Cyber Crime Coordination Centre (I4C)[9] backs up the NCRP, acting as the main hub for preventing, spotting, and investigating cybercrime across India.

CERT-In (Indian Computer Emergency Response Team)

CERT-In (the Indian Computer Emergency Response Team) plays a huge role in India's fight against cybercrime. Set up under the Information Technology Act, 2000[10], this team leads the charge whenever there's a cyber-incident. They don't just respond they also send out alerts, share updates about new vulnerabilities, and lay out best practices so everyone's on the same page. Service providers, intermediaries, and organizations are required to report any major cyber incidents, which helps CERT-In keep a pulse on threats as they happen.

Backing up CERT-In, you've got cyber forensic labs at both central and state levels. These labs jump in to collect, preserve, and analyze digital evidence essential steps if you want to actually prosecute cybercrimes, not just chase them around. Together, they form the backbone of India's cybercrime response.

Both central and state governments have rolled out a number of steps to boost cyber resilience. The central government[11] pushed for cybercrime police stations, set up cyber cells, and built special cyber units right into regular police forces. States teamed up with central agencies and brought in tech-driven investigation tools, digital evidence systems, and ways for states to share information with each other. On top of that, they've put together policies to protect critical information infrastructure and keep digital governance secure, all to tackle weak spots in the system.

An important dimension of institutional response efforts is capacity building and awareness programs. In cognizance of the fact that cybercrime is a challenge that is not only technical in nature but also human-centric, the government has made efforts to train law enforcement officials, prosecutors, and judicial officers on cyber laws, digital forensics, and emerging technology risks. Workshops, certification courses, and training modules are conducted on a regular basis through national and state police academies. Simultaneously, public awareness campaigns, including digital safety programs, school and college outreach programs, and mass media campaigns, are undertaken to sensitize citizens on safe online behavior, fraud prevention, and reporting mechanisms.

Judicial Approach:

Indian cyber law has evolved through historic Supreme Court decisions that have established the fundamental cyber rights and recent High Court decisions that have addressed

[9] Indian Cybercrime Coordination Centre (I4C) was established by MHA, in New Delhi to provide a framework and eco-system for Law Enforcement Agencies (LEAs) for dealing with Cybercrime in a coordinated and comprehensive manner.< https://i4c.mha.gov.in/> accessed 16 January 2026

[10] The Information Technology Act, 2000 § 70B

[11] Central Government has established a National Cyber Crime Reporting Portal which is working under the Ministry of Home Affairs < https://cybercrime.gov.in/Webform/Crime_NodalGrivanceList.aspx> accessed 18 January 2026

contemporary cybercrimes. A brief overview of some of the most important cases and their effects:

Lee Kun Hee v. State of Uttar Pradesh (2012)[12], the key issue involve in this case was whether the Indian criminal courts had the territorial jurisdiction over a foreigner in a case where the manufacturing and decision-making process occurred outside the boundaries of India. The petitioner challenged the criminal case against him before the Supreme Court on the grounds of lack of jurisdiction and the absence of direct personal involvement. The Supreme Court held that criminal prosecution must have a definite territorial nexus and specific allegations of personal involvement, and that mere occupancy of a high corporate position abroad is not sufficient to establish criminal liability within India. The Court therefore struck down the criminal case.

Swami Ramdev v. Facebook Inc. (2019)[13], the important question involve this case was whether the Indian courts had the ability to assert jurisdiction over the content of a foreign social media site (Facebook) that was allegedly causing harm to Indians in India when the content that was created or hosted outside of India, but was potentially harmful to Indians, could be governed by the laws of India. The Supreme Court of India examined the applicability of the "effects doctrine" in this case and held that the court have jurisdiction to try the cases when the consequences of the online content arises in India.

In the case of **Suhas Katti vs. State of Tamil Nadu (2004)[14]**, the Madras High Court held the accused liable for sending obscene and defamatory emails under the IT Act, 2000. The Court stated that sending obscene or defamatory electronic messages falls within the purview of Sections 66 and 67 of the IT Act. The Court clarified that cyber harassment and defamation are criminal offenses and that the identity of the sender can be proved by cyber forensic evidence. This case is a landmark decision in the prosecution of cybercrimes in India.

In **Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy & Anr. (2009[15])**, the main question was whether the Delhi High Court had territorial jurisdiction over an online dispute regarding trademark infringement merely because the defendant's website was accessible in Delhi.

The Delhi High Court held that mere accessibility of the website within a certain territory cannot by itself give rise to jurisdiction. The Court held that jurisdiction shall be attracted only if the defendant has targeted or conducted business within the forum state and if the cause of action has arisen within the forum state. The decision has been hailed as a landmark precedent on territorial jurisdiction in cyber and internet-related disputes in India by formulating the "purposeful availment" and "effects" tests.

In the case of **Shreya Singhal v. Union of India (2015)[16]**, the Supreme Court of India

[12] Lee Kun Hee v. State of Uttar Pradesh AIR 2012 SC 1007
[13] Swami Ramdev v. Facebook Inc. AIR 2020 (NOC) 529 (Del.)
[14] State of Tamil Nadu vs. Suhas Katti (C No. 4680 of 2004)
[15] Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy & Anr. 2009 SCC OnLine Del 3780
[16] Shreya Singhal v. Union of India, AIR 2015 SC 1523

declared Section 66A of the Information Technology Act, 2000, to be unconstitutional. The Court held that the provision was too vague and wide, thus violating the right to freedom of speech and expression under Article 19(1) (a) of the Indian Constitution. The Court held that the use of undefined terms such as **"offensive"** and **"annoying"** that allowed an arbitrary action had a chilling effect on the freedom of speech. However, the Court upheld the validity Section 69A in regard to blocking of websites and Section 79 with regard to the liability of intermediaries, provided that appropriate procedural protections have been followed.

Courts in India have slowly adapted the pace with challenges and the rise of cybercrimes and the tricky world of electronic evidence. As technology keeps moving forward, judges see the need to read the Information Technology Act, 2000, in line with older criminal laws so they can actually tackle new-age crimes. Over time, courts have made it clear that electronic evidence are recognised under the Indian Evidence Act, as long as it meets all the rules for being real and trustworthy. They've also stressed just how important it is to keep a clear chain of custody and follow Section 63 of The Bhartiya Sakshya Adhiniyam, 2023, which talks about the admissibility of the electronic evidence. Through several important cases, the courts have cleared up confusion around cybercrimes, settle down the rules for admissibility electronic evidence, and helped prosecutors go after digital offenders more easily. Further courts also emphasized issues like protection of personal data, liabilities of the intermediaries and how the cyber laws are aligned with the rights of the persons. Keeping all the things into consideration, the Indian courts trying to counter the challenges, which are emerging due the emerging trends of the cybercrime with the development of the new and advanced technologies which help the attacker to commit the cybercrime in cyber world? To deal these challenges in present day the courts are generally using purposive interpretation of the cyber laws.

Conclusion and Policy Recommendations:

Legal and Policy Recommendations:

i. Enact strong, tech-neutral cyber laws that actually keep up with new threats like AI scams, deepfakes, and cyber terrorism etc.

ii. Set up special cyber courts and a fast-track process so cases disposed in very short period of time and more criminals actually get convicted.

iii. Make it easier to go after cybercriminals abroad by strenthening up extraterritorial treaties.

iv. It required by time to setup digital forensic infrastructure and get all investigating agencies work in cooperation with each other. Incorporate specific statutory provisions on the collection, preservation, and admissibility of electronic evidence.

v. Enhance the accountability of the intermediaries while there is violation of freedom of speech and expression and privacy rights.

vi. Increase cyber awareness, education, and prevention efforts to lower cyber victimization rates and promote early reporting of crimes.

vii. Establish standard operating technological advanced tools for collecting, preserving, and analyzing digital evidence.

viii. Improve and expand Mutual Legal Assistance Treaties (MLATs) to enable faster international investigations and exchange of evidence.

Author's stance:

i. Cybercrime reporting systems and grievance redressal mechanisms should be improved and made simpler for victims to access easily and timely.

ii. There should be a comprehensive cyber law that should cover emerging trends of the cybercrime.

iii. Victim support services, such as counseling and legal aid should be provided to victims promptly and also insures the protection of personal data and privacy.

iv. Cyber awareness campaigns should be increased to prevent victims of cybercrimes.

v. Action should be taken strongly to remove content that is harmful to victims on the internet.

vi. There should be collaboration between law enforcement agencies, internet intermediaries, and civil society groups to prevent and respond to cybercrimes effectively.

Conclusion:

Cybercrimes in India keep changing shape of the legal system, so the law should be aligned with the new emerging trends of the cybercrime. New developing cybercrimes includes cyber fraud, ransomware, deepfakes, to tackle these crimes is very difficult because criminals are operating from the across borders. The government has tried to tackle these issues, but technology moves fast it is very big challenge for the government also to address these challenges because the system often lags behind. What India really needs now is a thorough, tech-savvy approach to cyber law. That's the only way to keep people safe online and make sure everyone's rights stay protected in this digital world.

References:

1. The Information and Technology Act, 2000
2. The Bhartiya Nayay Sanhita, 2023
3. The Bhartiya Sakshay Ashiniyam, 2023
4. Lee Kun Hee v. State of Uttar Pradesh AIR 2012 SC 1007
5. Swami Ramdev v. Facebook Inc. AIR 2020 (NOC) 529 (Del.)
6. State of Tamil Nadu vs. Suhas Katti (C No. 4680 of 2004)
7. Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy & Anr. 2009 SCC OnLine Del 3780

8. Shreya Singhal v. Union of India, AIR 2015 SC 1523
9. https://cyberpolice.nic.in/ accessed 12 January 2025
10. https://www.digitalindiaportal.co.in/about.php accessed 13 January 2026
11. https://cyberpolice.nic.in/ accessed 15 January 2026
12. https://i4c.mha.gov.in/ accessed 16 January 2026
13. https://cybercrime.gov.in/Webform/Crime_NodalGrivanceList.aspx accessed 18 January 2026
14. ICT Cyber Desk, 'Cyber Crime and Cyber-Terrorism, January-March 2016' (International Institute for Counter -Terrorism (ICT) 2016): https://www.jstor.org/stable/resrep09466.6 accessed 22 January 2026.