15 Conceptualizing Cyberspace and the Growing Challenge of Cybercrime in India

Dr. Balbir Kaur[1*] & Dr. Pankaj Kumar[2]
[1,2]Associate Professor, Kirori Mal College, University of Delhi.
*Corresponding Author: Preeti_balbir@yahoo.co.in

Abstract

The present study examines the contemporary cybersecurity landscape in India by reviewing major cyber threats, legal and institutional frameworks, and recent cyber incidents affecting both public and private sectors. By analysing representative case studies and existing cybersecurity measures, the study identifies key challenges in the current cybersecurity ecosystem and highlights opportunities for improving organizational preparedness and national cyber resilience. The findings are expected to contribute to the growing body of knowledge on cybersecurity governance while providing practical insights for policymakers, organizations, and researchers.

Keywords: Cyberspace, Cybercrime, Cybersecurity, Policymakers, Researchers, Case Studies.

Introduction

Just as advanced transportation systems necessitate the integration of automobile design and urban planning, the rapid evolution of information and communication technologies has made opting in to and participating in the global economy synonymous with offering services and conducting business in cyberspace. Everyone from governments, businesses, educational institutions and healthcare providers to individuals relies on cyberspace to communicate, transact, deliver services, and share or access information. In India, the Digital India program and its associated services like digital banking, e-governance, the Unified Payments Interface (UPI), and a host of other services have integrated digital technologies into the everyday lives of its citizens. All of these have been a boon to the economy and have provided a significant increase in the availability of services (Nandhini & Shanmuga Priya, 2026; Singh & Rathi, 2021).

The flip side of this digital boon is that as systems become even more interconnected, new cybersecurity challenges emerge. The increasing volume of interactions and transactions in the digital world have created new opportunities and

systems for malefactors to exploit human and technological systems. It is now safe to say that within the context of the digital world, the most significant threat faced by governments and businesses, and the most disconcerting threat faced by the citizenry, is cybercrime (Morgan, 2020). The nature of cybercrime is such that the digital criminal can operate anonymously and system jurisdictional boundaries thereby making its prevention, investigation and prosecution an unprecedented challenge.

The digital world has made it possible for crimes to be perpetrated through communication networks, computers and digital devices by making them the target and the medium of the crime.These actions consist of phishing, identity fraud, online scams, cyber stalking, ransomware, illegal intrusion to IT systems, data stealing, and assaults on vital infrastructures. In the past, cybercrimes consisted of a series of singular attempts to attack people. In the present, systems have sold the singular attempts to attack people and have thus become organized criminal structures, and in some cases, have the sponsorship of governments. These focuses have now even widened their range to include criminal enterprises that attack other organizations that manage sensitive and potentially harmful personal, financial, and strategic data, which is now even more sensitive, such as banks, hospitals, schools, various arms of the government, and large business firms (Singh & Rathi, 2021).

The Indian digital framework consists of numerous and large points of intersections that include first time and even novice users as a result of a decade of systematic multi-level efforts to include large and diverse groups of users that have created numerous points of intersections. At the same time, the substantial growth has occurred and continues to expand the range of connected payment systems, cloud computing, and social media. Even though it is a good thing for all connected systems to continue to grow and integrate to include more users as a means of achieving social and economic development, from all of the above, it is clear that connected systems have grown to the point that even the most novice of users have a good understanding of social and economic systems that need to be connected for development. Because of this expansion, the growth of connected systems means that the relative importance of systems connected for social and economic development is no longer simply the concern of the field of technology (IBM Security, 2024; Nandhini & Shanmuga Priya, 2026).

An increasing number of scholars believe that cybercrime is a socio-technical problem as opposed to a problem that is purely based on technology. Although sophisticated technologies enable cyberattacks, many successful breaches occur because of human factors such as weak passwords, negligence, lack of cybersecurity awareness, excessive trust, or failure to follow basic security practices. This perspective highlights the need to complement technological safeguards with

ISBN: 978-93-49468-66-5

behavioral interventions, cybersecurity education, and stronger organizational security cultures.

Threats of Cybercrime on Indian and Global Economy

Many successful cyberattacks happen as a result of insufficient and careless implementation of basic cyber hygiene. This can include use of weak passwords, accidental credential sharing, social engineering, and trusting cyber safety principles too much and ignoring the rules. It is important to physically implement systems and their supporting technologies to create behavior norm changes in the organization focused on fortifying cyber safety. Cybercrime victimizes people on a much bigger scale other than just the petty theft of money. Cybercrime has become the most expensive crime in the world and a critical threat to the global economy beyond just business and public service disruptions. The World Economic Forum (2025 Report) estimates that the cost of cybercrime will reach US$10.5 trillion per year making it the most expensive crime in the world. For businesses, the cost of cybercrime includes theft, fraud, and the direct and indirect costs associated with disappearing customers. This includes provision, legal, financial, and reputational costs, loss of business, and extended operational shutdowns (Morgan, 2020, World Economic Forum, 2025).

All businesses, without exception, are dealing with the emerging costs of cybercrime. The complexity of the crime is evident in the dramatic rise in the cost of the average data breach as documented in the IBM Security (2024 Report) data, which reports it as US$4.88 million. The crime shows most effect in the healthcare sector. The high sensitivity of healthcare data and its crucial nature drive the cost of average data breaches in healthcare to US$9.77 million, making it the most impacted sector globally (IBM Security, 2024).

There are emerging threats to the Indian economy from newly developing cyber infrastructure. The rapid digitalization of India has integrated technologies into systems like banking, financial services, healthcare, education, retail, telecommunication, manufacturing, and public administration. Digital technologies have made great positive changes to systems by providing access to more people. However, this has exposed more systems to greater risks of cyber threats. Digital financial fraud, phishing attacks on consumers, identity theft, ransomware for healthcare attacks, and breaches of government databases have all become common. Small and medium enterprises have very basic cyber protection, if any, and are therefore at great risk.

There is growing evidence to suggest that increases in cybercrime are not only a result of technological vulnerabilities. To improve cybersecurity, the focus must be shifted from technological restraints to the education of the users of the systems, workplace awareness, and the promotion of behavioral change. The use of Generative Artificial Intelligence (GenAI) also presents a new challenge. Cyber

ISBN: 978-93-49468-66-5

criminals will be able to use AI technologies to commit crime that will quickly and easily produce very real and very convincing phishing messages, fake web pages, and create convincing audio and video messages, among other things. The rapid advances in technology will blur the line between real and fake digital messages, making cybercrime even more successful. Organizations will also be able to use AI to commit crime against them. The counteracting of the crime monopolization of AI makes the focus on Cybercrime of the utmost importance.

Thus, it can be said that cybercrime is not merely a technological issue but a multidimensional challenge with many economic, social, organizational, and behavioral implications. A country like India, where digital transformation is progressing at an unprecedented pace, strengthening cybersecurity requires a balanced approach that combines technological safeguards, strong regulatory frameworks, organizational support, and enhanced cybersecurity awareness among people. Such a multi-dimensional approach is essential for building trust in the digital economy and ensuring that the benefits of digitalization are not undermined by the growing threat of cybercrime.

Emerging Cyber Threats and Vulnerabilities in Critical Infrastructure

The nature of cyber threats has changed significantly over the past decade. Earlier, cyberattacks were largely limited to viruses, malware, and isolated hacking attempts. Today, cybercrime has evolved into a highly organized and financially motivated activity carried out by professional criminal groups, international syndicates, and in some cases, state-sponsored actors (Singh & Rathi, 2021). These attackers use advanced technologies, artificial intelligence, automation, and sophisticated social engineering techniques to exploit weaknesses in individuals, organizations, and national infrastructure. As a result, cyber threats have become more frequent, complex, and difficult to detect.

The increase in attacks against key systems is highly problematic. Critical infrastructures are those whose disruption would impact the national security, economic stability, or public welfare of the country. These include health, banking, telecommunications, transportation, energy, defense, and government systems. With increased digitization, these systems are even more appealing to cyber criminals as even a transitory disruption will mean millions of system users suffer financial losses and/or inconvenience. (Singh and Rathi, 2021)

A related concern is the increased reliance organizations have on third-parties and digital service providers. Most businesses today do not run a closed and fully managed service. Partnerships with cloud computing, software, payment, logistics and IT services are the norm. While this positively impacts service delivery, it also brings about a greater number of attack surfaces. One partner's weak security can easily be exploited to attack the entire network. Supply-Chain attacks are some

ISBN: 978-93-49468-66-5

of the most prolific and quickly evolving threats in cyber security. (Nandhini and Shanmuga Priya, 2026; World Economic Forum, 2025). It is evident that Cybersecurity today goes well beyond securing one's own systems and compels organizations to be vigilant about the security of external service partners.

Now, cybercriminals are increasingly exploiting human vulnerabilities in addition to technological ones. One of the most successful forms of cybercrime is social engineering. In social engineering attacks, victims are tricked into divulging sensitive information or coerced into money transfers. India has some of the most extreme examples including “digital arrest” scams. In this kind of scheme, perpetrators call victims impersonating officials of The Central Bureau of Investigation (CBI), Enforcement Directorate (ED), or other police and government officials. Victims are called by video and told they are under investigation for and involved with illegal activities, including money laundering and drug trafficking. Victims are bombarded with fake legal notices, arrest warrants, and other supporting materials in a psychological attack to force victims to transfer money to the perpetrator’s account (Kaushik, 2026).

Artificial intelligence has made the situation even worse. With the advent of Generative AI, tools that simplify and automate the creation of digital phishing attacks that include fake websites, scam messages, and fully cloned and deepfake digital/audio/video person creations have been unleashed. The technology is so powerful and appears so authentic that individuals may have great difficulty recognizing a phishing attack. Cybersecurity problems are no longer the sole domain of technology systems. They increasingly have the dimensions of behavioral, psychological, and organizational problems (PwC India, 2024). For optimum cybersecurity, the technologically advanced security systems must be complemented with heightened awareness of the public, intentional employee upskilling, and the promotion of digital literacy among end-users.

Institutional Responses, Legal Frameworks, and Cyber Risk Management in India

Recognizing the global cyberspace threat, almost every country has implemented both preventive and corrective laws, regulations, and institutions to enhance their cyber resilience. In India, the governance of cybersecurity has seen a significant improvement over the last two decades. This has been done in a way that effectively manages the emerging digital risks in the country while ensuring that the Indian cyber domain supports the country's digital economy (Singh & Rathi, 2021).

India has enacted a number of laws that aim to strengthen legal capacity. Each law provides the legal infrastructure to address some aspect of cyber offenses, electronic records, and digital transactions. However, cyber threats have developed at an unprecedented pace. Therefore, India's regulatory framework also must

ISBN: 978-93-49468-66-5

undergo constant and dynamic changes to meet the emerging digital challenges. A recent major improvement in this regard is the DPDP Act, 2023. It has introduced comprehensive provisions for the protection of personal data of individuals and the provisions that regulate the practices of organizations dealing with digital information (Singh & Rathi, 2021).

In addition, India has strengthened institutions against crimes in the cyber domain. The Indian Cyber Crime Coordination Centre plays an important role in coordinating cybercrime investigations and support and assist law enforcement agencies and facilitate information sharing among states. Similarly, the National Critical Information Infrastructure Protection Centre focuses on protection of critical sectors of the economy such as power, banking, transportation, defense and telecommunications from cyberspace threats (Singh & Rathi, 2021). In combination, these agencies strive to develop a clear strategy for the management of cyber risks at the national level.

Major Cyber Incidents in India: Lessons for Cybersecurity

- **AIIMS New Delhi Ransomware Attack (2022)**

One of the most significant cyber incidents in India occurred in November 2022, when the All-India Institute of Medical Sciences (AIIMS), New Delhi, suffered a major ransomware attack. The attack disrupted several critical hospital services, including patient registration, laboratory reporting, admissions, billing, and access to electronic medical records. As digital systems became inaccessible, hospital staff were forced to return to manual paper-based processes for several days, resulting in delays in patient treatment and administrative operations.

It is claimed that 3 to 4 crore patients' private and sensitive medical records, the protective value of the health care data, and the effect of the absence of adequate preparedness against cybersecurity attacks are all demonstrated by this attack. Weaknesses within the AIIMS system, such as the use of old technology and applications, the absence of regular and necessary updates and security patches, insufficient endpoint protection, and poor cybersecurity fundamentals, all contributed to the success of this attack (Nandhini & Shanmuga Priya, 2026). Due to the lack of cybersecurity insurance policies at AIIMS, the burden of the costs of the recovery, the restoration of the systems, and the amendment of cybersecurity measures on the public funds was on the institution. This incident was a lesson for India's Health Sector and emphasized the need for periodic security assessments, timely and necessary software updates, reliable backup mechanisms, and comprehensive cybersecurity policies for public institutions.

- **Air India Supply-Chain Data Breach (2021)**

Another relatively famous example is the 2021 Air India data breach. Most cyberattacks aim to steal sensitive information by accessing a company’s internal

ISBN: 978-93-49468-66-5

systems. This breach occurred by accessing SITA, an international IT service provider who manages passenger service systems of a large number of airlines globally (Nandhini & Shanmuga Priya, 2026). As a result of the breach, private information of over 4.5 million passengers was affected, including their full names, details of their passports, their contacts, records of their tickets, information of their frequent flyer programs, and some information related to the payment cards.

The Air India case demonstrates that an organization can be a victim even if its own internal cybersecurity systems are intact. This case focused on the growing importance of the management of third-party vendors, ongoing security assessments, and contractual requirements of cybersecurity for external service providers (World Economic Forum, 2025). Unlike AIIMS, Air India successfully availed its cyber insurance to fund forensic investigations, legal compliance, customer notifications, and security improvements after the breach. This case illustrates the potential loss reduction impact of cyber insurance, while emphasizing that for an organization, strengthening cybersecurity across its entire digital supply chain is more important than strengthening only its internal systems.

- **Digital Arrest Scams: The Human Dimension of Cybercrime**

While ransomware attacks and data breaches generally affect organizations, cybercriminals are increasingly targeting ordinary citizens through sophisticated financial scams. One of the most alarming examples in India is the rise of "digital arrest" fraud (Kaushik, 2026). In these scams, fraudsters pose as officials from agencies such as the Central Bureau of Investigation (CBI), Enforcement Directorate (ED), police, or customs authorities. They contact victims through phone or video calls, falsely claiming that their bank account or identity has been linked to criminal activities such as money laundering or drug trafficking. To create panic and gain the victim's trust, they often display fake arrest warrants, forged legal documents, or fabricated evidence, forcing victims to stay connected on video calls while demanding immediate transfer of money for so-called verification or investigation purposes.

A widely reported case involved an elderly couple from Haryana who lost more than ₹1.05 crore after being manipulated and intimidated by fraudsters (Kaushik, 2026). The growing number of such incidents attracted the attention of the Supreme Court of India, which took *suomotu* cognizance of the issue. The Court emphasized the need for stronger coordination among the Reserve Bank of India (RBI), commercial banks, law enforcement agencies, and the Indian Cyber Crime Coordination Centre (I4C). It also encouraged measures such as e-Zero FIR registration, temporary freezing of suspicious bank accounts, and faster mechanisms for recovering money transferred through fraudulent transactions.

The increasing prevalence of digital arrest scams shows that cybercriminals are relying more on psychological manipulation than on technical expertise. Instead

ISBN: 978-93-49468-66-5

of exploiting weaknesses in computer systems, they exploit fear, confusion, and lack of awareness among people. This changing nature of cybercrime highlights that technological solutions alone cannot ensure cybersecurity. Public awareness campaigns, digital literacy programmers, financial awareness, timely law enforcement action, and better coordination among government agencies are equally important to protect citizens from such frauds.

Taken together, these case studies demonstrate that cyber threats can affect governments, organizations, and individuals alike. They also show that building a secure digital ecosystem requires a balanced approach that combines robust technological safeguards, effective legal and regulatory frameworks, organizational preparedness, cyber insurance, and continuous public awareness. As India's digital economy continues to expand, strengthening cybersecurity through collaboration between government institutions, businesses, and citizens will be essential for improving long-term digital resilience.

Discussion and Implications

With the growing economy of India, cyber security has turned into a serious issue for the country. The review of the literature on this topic and cyber incidents shows that cybersecurity is becoming an issue of governance and economy in India. This is clearly illustrated by the increasing amount of cyber-attacks on governmental institutions, companies, health organizations, and individuals. Thus, cybersecurity issues represent not an incident, but the process of development of constantly changing threats (Nandhini & Shanmuga Priya, 2026; Singh & Rathi, 2021).

Case studies analyzed in the paper show that there are numerous sources of cybersecurity vulnerability in different institutions. The examples of AIIMS ransomware and Air India data breaches indicate that such problems as outdated systems, slow software updates, and reliance on third-party services can lead to disruption of critical services and disclosure of sensitive information (Nandhini & Shanmuga Priya, 2026; World Economic Forum, 2025). At the same time, the growth of "digital arrest" scams indicates that cybercriminals utilize more and more psychological manipulations that cause people's trust and fear instead of just using technical skills (Kaushik, 2026). Thus, it can be concluded that modern cybersecurity needs both technical measures and people's awareness.

There are numerous initiatives aimed at developing of cybersecurity in India implemented in recent years. These include institutions like Indian Computer Emergency Response Team (CERT-In), the National Critical Information Infrastructure Protection Centre (NCIIPC), the Indian Cyber Crime Coordination Centre (I4C), and Cyber Swachta Kendra. Also, the legislative reform in the sphere of cyber security includes the introduction of the Digital Personal Data Protection Act, 2023 and new CERT-In reporting guidelines (Singh & Rathi, 2021). However, the

ISBN: 978-93-49468-66-5

implementation of these initiatives is inconsistent in some fields due to insufficient funding, lack of professionals, outdated infrastructure, and poor security culture in many organizations and public institutions.

The results of this research can provide useful recommendations for policymakers, organizations, and law enforcement bodies. In terms of the policy, the problem of cybersecurity needs to be recognized as a strategic goal rather than an IT issue. Organizations need to switch from the reactive approach that implies the response to cyber incidents to the risk-based approach that includes constant monitoring, security audit, timely software update, and Zero Trust principle (PwC India, 2024).In the same way, cybersecurity needs to be made an inseparable part of governance where senior management members get involved in cyber risk assessment and decision-making processes.

In the case of law enforcement, more institutional strength is required to deal with the increasing complexity of cybercrime cases. The establishment of a cybercrime unit in all states equipped with software developers, ethical hackers, digital forensic analysts, and legal professionals would greatly enhance their investigative powers (Singh & Rathi, 2021). Coordination between banks, regulatory bodies, law enforcement and institutions like I4C could help in minimizing financial losses by quickly freezing suspicious transactions and recovering lost funds (Kaushik, 2026).

Lastly, cybersecurity awareness needs to be made a national-level priority. As many of the cyber incidents take place because of mistakes made by humans and social engineering, raising awareness amongst citizens, employees and students about the right usage of technology would greatly minimize cyber threats.

Conclusion

Over the past years, India has made considerable progress in formulating major policies for cyber-security and developing institutions, and legal frameworks for combating the growing number and complexity of cyberattacks. But, still there remainsan important gap between policy formulation and effective implementation (Singh & Rathi, 2021; World Economic Forum, 2025). The most vulnerable sectors among all are SME's and Public sector organizations as they often operate with limited financial resources, outdated technological infrastructure, and insufficient cybersecurity expertise.

Therefore, it has now become extremely important to take more initiatives such as Digital India, Online Banking, Digital Payments via UPI, Mobile Wallets, e-governance, and smart technologies, protecting digital infrastructure and personal information has become increasingly important. The current study concludes that now-a-days cyber threats are becoming more advance and sophisticated, affecting

ISBN: 978-93-49468-66-5

more and more ordinary citizens, businesses and government institutions. (Singh & Rathi, 2021).

Although India has already set up important institutions like Institute of Information Security (Mumbai), RedTeam Hacker Academy (Bangalore/Multiple hubs), Craw Security (Delhi) and introduced significant reforms for strengthening cybersecurity, it still requires more effective implementation, continuous investment in technology, and greater collaboration among government agencies, private organizations, financial institutions, and citizens. There is an equalimportant need for developing cybersecurity awareness and digital literacy, as informed users remain the first line of defense against many cyber threats. There is a need of a balanced approach combining technology and legislation with the help of advanced technology, skilled professionals, effective law enforcement, and public awareness. It will be helpful in building a secure and resilient digital ecosystem which will further address future cybersecurity challenges (Nandhini & Shanmuga Priya, 2026; World Economic Forum, 2025).

References

1. IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation.
2. Kaushik, A. (2026, August 4). Supreme Court directs RBI, states & banks to implement urgent SOPs and money restoration measures to tackle "digital arrest" scams. Verdictum.
3. Morgan, S. (2020, November 13). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine.
4. Nandhini, A., & Shanmuga Priya, S. (2026). Case studies of major cyber incidents in India and the role of cyber insurance. In Proceedings of National Level Seminar on Cyber Insurance - Growth and Need for Cyber Security Coverage in India (pp. 155–159). Sri Ramakrishna College of Arts & Science.
5. PwC India. (2024). Digital trust insights: Cybersecurity trends in India. PricewaterhouseCoopers.
6. Singh, A., & Rathi, A. (2021). Current scenario of cyber-crime in India. International Journal of Law Management & Humanities, 4(1), 739–746.
7. Verizon. (2024). 2024 data breach investigations report (DBIR). Verizon Business.
8. World Economic Forum. (2025). Global cybersecurity outlook 2025. World Economic Forum.

☯☯☯

ISBN: 978-93-49468-66-5