International Journal of Criminal, Common and Statutory Law

E-ISSN: 2789-9500
P-ISSN: 2789-9497
IJCCSL 2025; 5(1): 04-07

www.criminallawjournal.org
Received: 04-10-2024
Accepted: 08-11-2024

Dr. Anuradha Chakraborty
Assistant Professor, Centre for Woman Studies and UNESCO Chair, Canada, Community Based Participatory Research Mentor of Sangawari Hub (CWS), Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India

Sanyogita Tiwari
Advocate Sanyogita Tiwari, Maharashtra, National Law University, Aurangabad, Maharashtra, India

Corresponding Author:
Dr. Anuradha Chakraborty
Assistant Professor, Centre for Woman Studies and UNESCO Chair, Canada, Community Based Participatory Research Mentor of Sangawari Hub (CWS), Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India

An analytical study on challenges and gaps in India's cyber security framework

Anuradha Chakraborty and Sanyogita Tiwari

DOI: https://doi.org/10.22271/27899497.2025.v5.i1a.110

Abstract
In the digital age, cyber security has emerged as a critical concern for nations worldwide, including India. As India emerges as a global digital powerhouse, its rapidly expanding digital landscape faces an unprecedented surge in cyber threats. From sophisticated state-sponsored espionage to disruptive ransomware attacks, the nation grapples with vulnerabilities that threaten its economic and national security. This paper delves into the critical shortcomings of India's cyber security framework, examining outdated policies, fragmented institutional mechanisms, and technological reliance on foreign solutions. By highlighting these gaps, the study advocates for comprehensive reforms to fortify India's resilience against an evolving spectrum of cyber threats.

Keywords: Cyber security, cyber bullying, cybercrime, jurisdiction

1. Introduction
The digital revolution in India, driven by initiatives such as "Digital India," has significantly transformed governance, businesses, and society. However, this rapid digitization has also exposed critical vulnerabilities in India's cyber ecosystem. Despite the introduction of policies like the National Cyber Security Policy (NCSP) 2013, India continues to face escalating cyber threats (Raghavan & Singh, 2021) [5]. In 2023, India ranked among the top ten countries most affected by cyberattacks (CERT-In, 2023) [7]. However, the cybersecurity framework has struggled to keep pace with this evolving threat landscape. This paper explores the challenges and gaps in India's cyber security framework, analyzing existing policies, technological shortcomings, and institutional deficiencies. The study underscores the urgent need for robust strategies to address emerging cyber threats and safeguard national security.
Cybercrime has emerged as a pressing issue in India, driven by the rapid adoption of digital technologies and an expanding internet user base. While digital connectivity has brought convenience, it has also exposed individuals, businesses, and governments to an array of cyber threats. There are many patterns of cybercrime, worldwide.

1.1 Some prevalent cybercrimes in India are-
a) Identity Theft
Identity theft involves stealing personal information such as Aadhaar details, PAN numbers, or financial credentials to commit fraud. With the growing digitization of government services and banking systems, cybercriminals exploit vulnerabilities to impersonate individuals and access their assets.

Examples
- Cloning of debit/credit cards.
- Phishing attacks targeting OTPs and passwords.

Impact
Victims often face financial losses and legal complications, while institutions suffer reputational damage.

b) Financial Frauds: Online financial scams are among the most reported cybercrimes in India. These include phishing, vishing (voice phishing), and fraudulent online transactions. Scammers often impersonate banks or financial institutions to deceive victims.

Recent Trends in financial frauds
- Fake investment schemes.
- Unauthorized UPI transactions.
- Crypto-based Ponzi schemes.

Mitigation: The RBI has intensified awareness campaigns to educate users on secure digital banking practices.

c) Cyberbullying and Online Harassment: Cyberbullying and harassment, especially on social media platforms, have escalated. Victims, often women and children, face threats, blackmail, or defamation.

Notable Cases
Instances of "morphing" (altering images/videos to defame) and trolling targeting prominent individuals have gained attention.

Legal Recourse
The IT Act, 2000, and specific sections of the IPC address online harassment, but enforcement remains a challenge.

d) Ransomware Attacks: Ransomware attacks have surged, targeting businesses, hospitals, and even government organizations. Attackers encrypt critical data and demand ransom for its release.

High-profile Incidents
- Attacks on Indian healthcare providers during the COVID-19 pandemic.
- Compromises in small and medium enterprises (SMEs).

Response
CERT-In (Computer Emergency Response Team - India) has issued guidelines for preventing and mitigating ransomware attacks.

e) Online Child Exploitation: The availability of the dark web and encrypted messaging platforms has facilitated heinous crimes like child pornography and exploitation.

Efforts
The National Cyber Crime Reporting Portal allows anonymous reporting of such crimes, and agencies like NCMEC collaborate with Indian law enforcement.

f) Cyber Espionage and Nation-State Attacks: Cyber espionage by foreign actors poses a threat to India's national security. Sensitive information related to defense, infrastructure, and government operations is often targeted.

Examples
- Malware attacks linked to state-sponsored groups.
- Attempts to compromise critical infrastructure like power grids.

Measures
India's National Cyber Security Policy emphasizes the need for robust cybersecurity frameworks and international cooperation.

g) Fake News and Misinformation: The dissemination of fake news, often through WhatsApp and other social media platforms, incites communal violence and disrupts social harmony.

Notable Instances
- Spread of fake COVID-19 cures.
- Misinformation during elections.

Counter actions
Social media companies collaborate with Indian authorities to curb fake news through fact-checking initiatives.

1.2 Gaps in Policy and Strategy
India's primary cyber security policy, the National Cyber Security Policy (NCSP) of 2013, is considered outdated and insufficient to address the dynamic nature of cyber threats. The policy lacks actionable objectives and clear implementation timelines (Sundararajan & Gupta, 2023) [8]. Moreover, it does not adequately address emerging technologies such as artificial intelligence (AI), the Internet of Things (IoT), and quantum computing, which have introduced new vulnerabilities into the digital ecosystem.

Another gap lies in the absence of a centralized authority to oversee and coordinate cyber security efforts across sectors. The current framework relies on multiple agencies, including the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC), leading to fragmented efforts and jurisdictional overlaps (Mishra *et al*., 2022) [4].

1.3 Inadequate Legal Framework
India's legal provisions for cyber security are primarily encapsulated in the Information Technology Act of 2000, which has undergone amendments but still falls short in addressing contemporary cybercrimes. For instance, the Act does not comprehensively cover issues such as data privacy, cyberbullying, and ransomware attacks (Sharma & Kumar, 2022) [9]. Additionally, there is a lack of stringent penalties for cyber offenses, which undermines deterrence.

The absence of a robust data protection law further exacerbates the problem. Although the Digital Personal Data Protection Act, 2023, aims to address some of these concerns, its implementation and enforcement mechanisms remain unclear (Singh & Verma, 2021) [2].

1.4 Insufficient Infrastructure and Resources
India's cyber security infrastructure is inadequate to handle the growing scale and sophistication of cyber threats. There is a shortage of skilled cyber security professionals, with demand far outstripping supply (Nasscom, 2021). Furthermore, small and medium enterprises (SMEs), which constitute a significant portion of India's economy, often lack the resources and expertise to implement robust cyber security measures.

Critical infrastructure sectors such as power, banking, and healthcare are particularly vulnerable due to outdated systems and inadequate investment in cyber security. For example, a report by the Data Security Council of India (DSCI) highlighted that over 60% of Indian organizations have experienced cyberattacks targeting critical infrastructure in recent years (DSCI, 2022).

1.5 Limited Public Awareness
Public awareness about cyber security remains low in India, making individuals and organizations susceptible to

cyberattacks. Phishing scams, identity theft, and social engineering attacks are prevalent, largely due to the lack of education and awareness campaigns (Rao *et al.*, 2023) [12]. Efforts to promote cyber hygiene and safe online practices have been sporadic and limited in reach.

2. Research Methods

The study was conducted as a purely analytical review, focusing on various research articles, reports, and other scholarly resources related to cybercrime. The primary sources of data were reputable academic databases, including Google Scholar, Web of Science, and other relevant platforms known for their extensive collections of peer-reviewed literature. Articles were selected based on their relevance, quality, and contribution to the existing body of knowledge on cybercrime.

A systematic approach was adopted to identify, assess, and synthesize the literature. Keywords such as "cybercrime," "cybersecurity," "digital threats," and "online fraud" were used to perform comprehensive searches across the selected databases. To ensure inclusivity and relevance, the search criteria were limited to publications within the past 10 years, unless older articles were deemed foundational or particularly significant to the topic.

Each selected article was critically analyzed to extract information on themes such as the types of cybercrimes, emerging trends, regional and global impacts, preventative measures, and policy implications. The findings were then categorized and compared to identify patterns, gaps, and areas for future research. This method allowed for a thorough understanding of the current state of knowledge while also highlighting key challenges and opportunities in the field.

By relying on established sources and employing a structured review process, this study aimed to ensure the reliability, validity, and comprehensiveness of its findings.

3.Review of Studies on Lacuna in Indian Cybersecurity

India, as one of the fastest-growing digital economies, faces significant challenges in the domain of cybersecurity. Numerous studies have highlighted critical gaps in India's cybersecurity framework, policies, and preparedness. This review synthesizes the key findings from these studies, categorizing the lacunae and proposing potential pathways for improvement.

a) **Policy and Regulatory Gaps:** Many studies point to the inadequacy of India's cybersecurity policy framework. The National Cyber Security Policy (NCSP) of 2013, although a foundational document, is considered outdated given the rapidly evolving threat landscape. There is a lack of a comprehensive and updated cybersecurity policy addressing emerging threats such as ransomware, AI-based attacks, and IoT vulnerabilities. Researchers have called for a more dynamic and actionable policy framework, akin to those adopted by countries like the United States and Singapore.

   India's NCSP 2013 has been criticized for being outdated and inadequate in addressing emerging threats such as ransomware, advanced persistent threats (APTs), and Internet of Things (IoT) vulnerabilities (Mishra & Sharma, 2022) [4]. Moreover, there is limited public-private collaboration, which is vital for sharing threat intelligence and building a robust security infrastructure (Bhatia, 2020) [1].

b) **Critical Infrastructure Protection:** India's critical infrastructure, including power grids, banking systems, and public utilities, remains a prime target for cyberattacks. Studies reveal significant vulnerabilities in these systems due to outdated technologies, limited adoption of international security standards, and insufficient coordination between public and private entities. The ransomware attack on the AIIMS hospital in 2022 underscored the critical gaps in securing healthcare infrastructure.

c) **Human Resource Challenges:** Another major lacuna highlighted by studies is the acute shortage of skilled cybersecurity professionals in India. Despite the growing demand for expertise in threat detection, vulnerability assessment, and incident response, the country faces a talent deficit. Initiatives like the Cyber Surakshit Bharat program, while commendable, are insufficient in addressing this gap. There is an urgent need to integrate cybersecurity education into mainstream curricula and incentivize skill development through government-industry partnerships.

d) **Technological and Research Deficits:** India lags behind in the development and deployment of indigenous cybersecurity technologies. A heavy reliance on imported solutions exposes the nation to supply chain vulnerabilities. Furthermore, the lack of dedicated funding and infrastructure for cybersecurity research limits innovation in combating sophisticated threats. Studies suggest that fostering a startup ecosystem focused on cybersecurity could mitigate this challenge.

e) **Public Awareness and Reporting Mechanisms:** Many studies emphasize the low levels of cybersecurity awareness among individuals and small businesses. Phishing attacks, identity theft, and financial fraud often succeed due to a lack of basic cyber hygiene practices. Additionally, the underreporting of cybercrimes due to fear of reputational damage or inadequate redress mechanisms hampers effective threat assessment.

f) **International Cooperation:** India's cybersecurity posture is further weakened by limited international collaboration. While the country is part of initiatives like the Global Forum on Cyber Expertise (GFCE), studies indicate that India must proactively engage in global cyber diplomacy to share intelligence, standardize practices, and build collective resilience against transnational cyber threats.

3.1 Challenges in India's Cyber Security Framework

The cyber security system in India has many strengths, including government initiatives, regulatory frameworks, skill development programs, and public-private partnerships. These positive aspects create a robust foundation for addressing current and future challenges, enhancing the country's cyber resilience, and ensuring secure digital growth. However, there are some gaps which are being worked on to create a safe environment in the country with respect to cyber security.

4. Results and Discussion

Results and discussion have been done under these following heads-

4.1 Policy and Legal Gaps
The NCSP 2013 lacks specificity and has not been updated to tackle emerging cyber threats. For instance, there are no clear guidelines for securing critical infrastructure sectors like healthcare and energy (Sharma, 2021) [6]. Additionally, India does not have a dedicated cyber security law, relying instead on the Information Technology Act, 2000, which has limitations in addressing modern threats.

4.2 Institutional framework for cyber security
India's institutional framework for cyber security suffers from fragmentation. Agencies like the Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), and others operate with overlapping mandates, leading to inefficiencies (Kumar *et al*., 2021) [3]. Moreover, there is a shortage of skilled cyber security professionals, which hinders the effectiveness of these institutions.

4.3Technological Deficiencies
India's reliance on imported technology poses a significant security risk. The lack of indigenous cyber security solutions makes critical systems vulnerable to backdoors and supply chain attacks (Raghavan & Singh, 2021) [5]. Additionally, inadequate investment in research and development (R&D) further exacerbates these vulnerabilities.

4.4 Awareness and Capacity Building
Public awareness of cyber security remains low, especially among small and medium enterprises (SMEs) and rural internet users. Cyber hygiene practices are rarely prioritized, resulting in increased susceptibility to phishing attacks, malware infections, and fraud (Gupta & Mehta, 2020) [1].

5. Recommendations
Recommendations of the present analysis are-

5.1 Policy Reforms
The NCSP must be revised to address modern threats, focusing on areas such as IoT security, cloud computing, and AI-driven attacks. A dedicated cyber security law should be enacted to streamline legal processes and establish clear accountability (Sharma, 2021) [6].

5.2 Institutional Strengthening
Greater coordination among agencies is essential to eliminate redundancies. Establishing a unified cyber security agency with overarching authority can enhance response mechanisms. Additionally, programs to train cyber security professionals should be prioritized to address skill shortages (Bhatia, 2020) [1].

5.3 Promoting Indigenous Technologies
Investing in R&D for indigenous cyber security solutions can reduce dependency on foreign technology. Initiatives like "Make in India" should focus on developing secure hardware and software for critical sectors (Mishra & Sharma, 2022) [4].

5.4 Enhancing Awareness and Training
Awareness campaigns targeting SMEs, educational institutions, and rural areas can improve cyber hygiene. Collaborations with tech companies to deliver workshops and training programs can bridge the knowledge gap (Gupta & Mehta, 2020) [1].

6. Conclusion
India's cyber security framework faces significant challenges, including outdated policies, fragmented institutions, and technological vulnerabilities. Addressing these gaps requires a multi-pronged approach involving policy reforms, institutional strengthening, technological advancement, and public awareness. By adopting these measures, India can build a resilient cyber security framework capable of safeguarding its digital ecosystem. The studies on lacunae in Indian cybersecurity present a sobering picture of the nation's preparedness against cyber threats. While significant strides have been made in recent years, addressing these gaps requires a multi-pronged approach involving policy reform, capacity building, technological advancement, and international collaboration. Given the increasing digitization of every aspect of Indian life, the urgency to bridge these gaps cannot be overstated. India's digital transformation has brought significant opportunities but also magnified the risks associated with cybercrime. While initiatives like the Digital India program aim to bridge the digital divide, they also highlight the need for robust cybersecurity measures. Strengthening laws, promoting cyber hygiene, and enhancing the capabilities of law enforcement are critical to countering the rising tide of cybercrimes in the country.

A collaborative effort between the government, private sector, and citizens can ensure a safer cyberspace for all.

References

1. Bhatia A. Public-private collaboration in cyber security: An Indian perspective. J Cyber Policy. 2020;5(2):101-119.
2. Gupta P, Mehta R. Cyber hygiene practices in India: Challenges and solutions. Indian J Inf Technol. 2020;12(3):45-58.
3. Kumar S, Mishra P, Singh A. Institutional challenges in India's cyber security landscape. Cyber Secur Rev. 2021;9(4):32-47.
4. Mishra V, Sharma R. Rethinking India's National Cyber Security Policy. Def Strateg Stud J. 2022;15(1):89-103.
5. Raghavan S, Singh K. Cyber resilience in India: Opportunities and challenges. Int J Cyber Stud. 2021;18(2):67-81.
6. Sharma P. Securing critical infrastructure in India: A cyber security perspective. Energy Policy Res Q. 2021;6(1):13-24.
7. CERT-In. Annual Cybersecurity Threat Report 2023. Ministry of Electronics and Information Technology; c 2023.
8. Gupta R. Challenges in Public-Private Cybersecurity Collaboration in India. Cybersecur J India. 2023;15(3):45-58.
9. Kumar A, Singh P. Institutional shortcomings in India's cybersecurity framework. Nat Cyber Stud. 2022;28(4):12-21.
10. Mehta V. Ransomware Attacks on Critical Infrastructure: The Indian Context. J Cybersecur. 2023;19(1):73-89.
11. Pillai S. Evaluating India's Digital Personal Data Protection Act. Legal Perspect Cybersecur. 2023;22(2):36-48.
12. Rao M. Cybersecurity Awareness in India: A Rural-Urban Divide. Econ Polit Wkly. 2023;58(7):18-25.
13. Sharma N. Bridging the Cybersecurity Skills Gap: India's Roadmap. NASSCOM Cybersecur Rep. 2023.