INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

BEYOND THE FIREWALL: UNRAVELING THE COMPLEXITIES OF INDIAN CYBERCRIME INVESTIGATIONS

AUTHOR - SHAMIK LODH, LLM SCHOLAR AT AMITY UNIVERSITY

BEST CITATION - SHAMIK LODH, BEYOND THE FIREWALL: UNRAVELING THE COMPLEXITIES OF INDIAN CYBERCRIME INVESTIGATIONS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (1) OF 2025, PG. 1274-1278, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

India is experiencing unprecedented growth in the digital space and, with that digital growth, comes unprecedented growth in the rate of cybercrime, which threatens national security, economic prosperity and public safety. This report addresses the various nuanced challenges of investigating cybercrime in India across five areas - allocating resources strategically, developing a legal framework for law enforcement, engaging in international coordination, gaining access to encryption technology, and providing specialized training.

The report notes that India has been making tremendous advances in building its cybersecurity infrastructure with vast amounts of funding, and positive legal frameworks, but that it still faces challenges, historically, of technical training, transnational coordination and specially trained personnel to respond to the demands of cyberspace. Addressing this will require a recognition that a collaborative response needs to involve the coordination of strong enforcement, privacy protections, and sharing of domestic, as well as international expertise.

Key words: *Cybercrime , Digital growth , National security , Economic prosperity , Public safety, Cybersecurity infrastructure.*

Introduction

Cybercrime has become a serious threat to national security, economic stability, and public safety in India. With the rising digitization and increased use of digital technologies and the internet, India has undergone significant vulnerabilities that people and groups are willing to explore. This paper discusses the technical and organizational challenges of investigating cybercrime in India. These challenges begin with the Strategic allocation of resources, legislative reform, international cooperation, privacy access protocols, and provisions for training when developing the basis for India's cybercrime responses.[2534]

Strategic Allocation of Resources

It is important to have a strategic allocation of resources to respond to cyber crime more effectively. India demonstrates the strategic allocation of financial and human resources directed towards advanced threat detection and monitoring tools, as well as incident response capabilities.[2535]

Financial Resources

India has allocated more than ₹1,550 crore in its budget to strengthen cybersecurity, combat cyber criminal activity and build out its AI-centric research capabilities. That kind of

[2534] www.ETCISO.in, *Legal Gaps and Concerns Abound as Cybercrime Rises Unabated in India - ET CISO*, ETCISO.IN, https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/legal-gaps-and-concerns-abound-as-cybercrime-rises-unabated-in-india/106434980 (last visited Mar 29, 2025).

[2535] Rajarshi Dhar, *Union Budget 2025 Prioritizes Cybersecurity Amid Rising Threats*, FROST & SULLIVAN (Feb. 4, 2025), https://www.frost.com/uncategorized/union-budget-2025-prioritizes-cybersecurity-amid-rising-threats/ (last visited Mar 29, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

financial resource demonstrates the country's strategic posturing of allocating financial resources in order to protect against cyber threats source . Additionally, the Ministry of Home Affairs allocated ₹131.60 crore under CCPWC in response to cybercrime against women and children source .[2536]

Technical Resources

By investing in newer technical resources, as well as the capability for continuous monitoring, organizations can gain a stronger security posture to reduce their risk of cyber incidents. This would include the capability to purchase advanced forensics machines and training for personnel to explore the latest threat vectors and best practices for defending against those vectors source .

Incident Response Capability

Proper allocation of resources allows cybersecurity personnel to stay ahead of advance potential threats, whether that is identifying breaches more quickly, or responding to incidents far more efficiently. For example, cyber fraud against citizens is on the rise (to the tune of 51% in the past year), pointing more directly to the need for effectiveness in allocating resources, as well as greater cybersecurity measures source.[2537]

Legislative Reforms

Legislative reforms play a pivotal role in addressing the evolving landscape of cybercrime. India has made significant strides in enacting laws and regulations to enhance data privacy and cybersecurity, creating a more robust framework for investigators and prosecutors.

Digital Personal Data Protection Act (DPDP Act) 2023

The DPDP Act of 2023 is India's first comprehensive data protection law. It introduces strict compliance requirements regarding the collection, processing, storage, and transfer of digital personal data. Key provisions include empowering citizens with data rights and imposing heavy penalties for violations (up to ₹250 crores) source .[2538]

Information Technology Act, 2000

The Information Technology Act, 2000, is the primary legislation governing cybersecurity and cybercrime in India. It includes provisions for data protection and handling breaches of confidentiality and privacy, particularly under Section 72A, which addresses unauthorized disclosure of personal information source .[2539]

Cybersecurity Regulations

The Indian government has drafted rules detailing how organizations must manage citizens' data privacy. These rules are designed to enhance the security framework for personal data and mitigate cyber risks source . These regulations provide investigators with clearer guidelines on data access while respecting privacy boundaries.[2540]

International Cooperation

International cooperation is necessary when fighting cybercrime which can easily cross international borders. In order to build cooperation in cybercrime investigations, India has entered into multiple agreements, treaties, and cooperation regarding international crime at the multilateral, regional, and bilateral treaty levels.

[2536] CXOtoday News Desk, *Indian Government Doubles Cybersecurity Funding from Rs 400 Cr to Rs 750 Cr in 2024 Interim Budget: Industry Leaders Strongly Advocate*, CXOTODAY.COM (2024), https://cxotoday.com/specials/indian-government-doubles-cybersecurity-funding-from-rs-400-cr-to-rs-750-cr-in-2024-interim-budget-industry-leaders-strongly-advocate/ (last visited Mar 29, 2025).

[2537] CHERIAN SAMUEL & MUNISH SHARMA, INDIA'S STRATEGIC OPTIONS IN A CHANGING CYBERSPACE (2019).

[2538] The Digital Personal Data Protection Bill, 2023, PRS LEGISLATIVE RESEARCH, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (last visited Mar 29, 2025).

[2539] it_act_2000_updated.pdf, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited Mar 29, 2025).

[2540] Cybersecurity Laws and Regulations Report 2025 India, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india (last visited Mar 29, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Convention on Cybercrime (Budapest Convention)

The Budapest Convention was created to provide general and specific cooperation measures as implemented to combat cybercrime. It allows practitioners from different countries that are a party to the convention to share information and experiences and develop strategies. While India is not a party to the Budapest Convention, the framework it provides influences international best practices, that Indian agencies are starting to adopt.[2541]

United Nations Convention against Cybercrime

This treaty was adopted by the UN General Assembly on December 24, 2024, to enhance international cooperation regarding cybercrime. The treaty strives to achieve equilibrium between law enforcement and the protection of privacy and human rights, while combating cybercrime. India's participation in the treaty is an indicator that they are committed to protecting and preserving the international community.[2542]

INTERPOL Initiatives

INTERPOL is working to enhance the capacity of member countries to prevent, investigate and disrupt cybercrime, and thereby protect their communities with regards to crime that crosses borders. India is active in this regard, being a participant in INTERPOL-led operations tackling various crimes, like financial fraud, exploitation of children, and ransomware.[2543]

Privacy Access Protocols

Protocols for privacy access are important for protecting both individuals and organizations' data and personal information from tactics used by bad actors in cyberspace. Privacy access protocols consist of policies, procedures, and technology that are used to protect computer systems, computer networks, and data from unauthorized access while allowing for possible legitimate investigative steps to take place.[2544]

Data Privacy and Confidentiality

Data privacy indicates who is able to access data, with data protection referring to the use of certain tools and/or policies to limit or prevent access from non-authorized persons. Confidentiality protects the data from unauthorized access, disclosure, and/or theft and preserves the rules of sensitive information access. (Cloudian, University of Delaware) Investigators in India must navigate these privacy protocols while engaging in a the legitimate investigative process.[2545]

Cyber Security Protocols and Best Practices

Cybersecurity protocols encompass the methods and techniques for safeguarding the protection of networks, systems, and data. Cybersecurity includes preventative measures and procedures for responding to incidents. (DataGuard, CISA) Indian police agencies have slowly begun adopting international standards of cybersecurity protocols and best practices to ensure their respective investigations are following international benchmarks for investigations.[2546]

Legal & Regulatory Frameworks

There are a number of rules that govern privacy on the internet that promote and protect a person's personal information and privacy while on the internet and/or while establishing standards for the protection of information and personal data against threats that exist on the internet. (Thomson Reuters). The legal and regulatory frameworks create tight boundaries that police investigators are expected to

[2541] Budapest Convention and related standards - Cybercrime, https://www.coe.int/en/web/cybercrime/the-budapest-convention-old (last visited Mar 29, 2025).

[2542] A_AC291_12_Adv.pdf, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/A_AC291_12_Adv.pdf (last visited Mar 29, 2025).

[2543] INTERPOL-led operation targets growing cyber threats, https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats (last visited Mar 29, 2025).

[2544] Internet Privacy in India — Centre for Internet and Society, https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india (last visited Mar 29, 2025).

[2545] Data privacy in the campus cloud - University Business, https://universitybusiness.com/data-privacy-in-the-campus-cloud/ (last visited Mar 29, 2025).

[2546] What is the Cybersecurity Information Sharing Act (CISA)?, WHATIS, https://www.techtarget.com/whatis/definition/Cybersecurity-Information-Sharing-Act-CISA (last visited Mar 29, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

monitor as they seek to pursue possible legitimate investigative avenues for digital evidence.[2547]

Specialized Training Programs

Cybercrime investigation specialization training aims to improve individuals' capacity to conduct effective investigations. These training programs frequently employ a blended approach, which consists of self-study, live tutors interactions, and instructor-led investigation exercises.[2548]

The National Cybercrime Training Centre (CyTrain)

CyTrain issues law enforcement officers with certifications like I4C Certified Specialist and I4C Certified Expert. These certifications will provide investigators with the technical know-how to analyze digital evidence and pursue the activity of cybercriminals CyTrain.[2549]

Indian Cybercrime Coordination Centre (I4C)

The I4C has developed a monthly series of workshops, which are technical sessions focused on new and emerging technologies are being used by cybercriminals that law enforcement must be aware of to effectively investigate, I4C Training page . These workshops will provide investigators with the knowledge and skills they will need to keep pace with new approaches to cybercrime and the technology cybercriminals are using.[2550]

The Cyber Commando Training Program

This is a governmental initiative and is aimed at developing a cyber investigator elite force to mitigate the complex threats arising from the digital world, IIT Kanpur - Cyber Commando page.[2551]

Cyber Shikshaa Program

This program is a flagship program aimed at training women engineering grads from tier-II and tier-III cities, or rural areas with cybersecurity skills to diversify the talent pool and inaugurate diversity to the cybercrime investigation role, Cyber Shikshaa.[2552]

Courses in Cyber Security from NIIT

NIIT has provided various options covering network security, ethical hacking, and incident response, along with offering practical cybersecurity skills to both public and private sector practitioners NIIT.[2553] .

EC-Council Cybersecurity Training

EC-Council has opportunities for various cybersecurity courses in India, including Certified Ethical Hacker and Certified Penetration Testing Professional, which are internationally recognized credentials for cybersecurity professionals EC-Council.[2554]

Challenges and Recommendations

Key Challenges

1. **Lack of Technical Capacity:** Many law enforcement agencies, especially at the local and state levels, have not made significant advancements toward specialized digital forensics training and equipment no matter how much funding has been provided.[2555]
2. **Jurisdictions Issue:** Evidence collection and prosecution are often complicated by jurisdictions in cybercrime investigations.[2556]

[2547] Internet Laws & Internet Regulation, / (2021), https://www.kaspersky.com/resource-center/preemptive-safety/internet-laws (last visited Mar 29, 2025).

[2548] CyTrain Portal | Education, https://en.vikaspedia.in/viewcontent/education/digital-litercy/information-security/cytrain-portal (last visited Mar 29, 2025).

[2549] Mandatory training for UP cops to tackle cybercrime, THE TIMES OF INDIA, May 10, 2022, https://timesofindia.indiatimes.com/city/lucknow/mandatory-training-for-up-cops-to-tackle-cybercrime/articleshow/91454423.cms (last visited Mar 29, 2025).

[2550] Cytrain Setu Virtual Event – 2022, https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1856890 (last visited Mar 29, 2025).

[2551] Mandatory training for UP cops to tackle cybercrime, *supra* note 16.

[2552] Union Home Minister and Minister of Cooperation, Shri Amit Shah launches e-Sakshya, Nyaya Setu, Nyaya Shruti and e-Summon App for three new criminal laws in Chandigarh today, https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=2041322 (last visited Oct 17, 2024).

[2553] CyTrain Portal | Education, *supra* note 15.

[2554] Cytrain Setu Virtual Event – 2022, *supra* note 17.

[2555] Teri Flory, *Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies*, JDFSL (2016), http://commons.erau.edu/jdfsl/vol11/iss1/4/ (last visited Mar 29, 2025).

[2556] Digital forensics, https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics (last visited Mar 29, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

3. **Evolving Cybercriminals:** Cybercriminals are always evolving, and investigators always must be learning and evolving their skills and tools.[2557]
4. **Privacy and Investigatory Needs:** The balance between privacy rights and investigatory needs has always been a challenge.[2558]
5. **Lack of Talent:** India is experiencing a severe lack of cybersecurity experts with investigative skills.[2559]

Recommendations

1. **Diversifying Capacity Development:** Invest in advanced technical capacity across Cybercrime Units at the state and district levels with targeted resourcing and funding.
2. **Public-Private Partnerships:** Formalize partnerships that exist across law enforcement and the private sector cybersecurity response professionals to maximize the benefit of the expertise available across industry.
3. **Judicial Training:** Develop programs for judges and prison prosecutors to increase knowledge of digital evidence and cyber crime investigations.
4. **International Protocols:** Move forward with the development of international protocols for sharing of cross-border evidence and collaborative investigations.
5. **Academic Integration:** Integrate and develop cyber crime investigation modules into computer science and law programs in order to develop the next generations of cyber crime investigators.

Conclusion

Cybercrime poses a real national security, economic stability, and public safety threat to India. Responding to these threats will require a coordinated approach which maximizes resource allocation, legislative change, international co-operation, access to data solutions, and education. Harnessing information technology, improved data protection legislation, and international co-operation plus education of cybersecurity Professionals will strengthen India's defence against the cybercrime threat. The journey ahead for India will not be easy as criminals are becoming increasingly sophisticated, and India must remain vigilant and adaptive. Success will depend on how well India can find the right balance between policing and protecting privacy; building domestic capacity and developing international contacts. If India maintains focus on these pillars it will secure access to cyberspace for its citizens and business.

[2557] UNODC Strengthens Philippine Anti-Corruption and Law Enforcement Agencies' Capacity in Digital Evidence Collection and Processing, https://www.unodc.org/roseap/what-we-do/anti-corruption/topics/2023/11-digital-forensics-training.html (last visited Mar 29, 2025).

[2558] Digital forensics, *supra* note 23.

[2559] Scott H Belshaw, *Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education*, 2019 JOURNAL OF CYBERSECURITY EDUCATION, RESEARCH AND PRACTICE (2019), https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/3 (last visited Mar 29, 2025).