Stallion Journal for Multidisciplinary Associated Research Studies
ISSN (Online): 2583-3340
Volume-4 Issue-2 || April 2025 || PP. 315-319 https://doi.org/10.55544/sjmars.4.2.21

Strengthening Global Cybersecurity: India's Engagement in International Cybercrime Control

Dr Ajay Pratap
AP-III, AIIT, Amity University Uttar Pradesh Lucknow, INDIA

Corresponding Author: apratap@lko.amity.edu

www.sjmars.com || Vol. 4 No. 2 (2025): April Issue

Date of Submission: 02-04-2025	**Date of Acceptance:** 13-04-2025	**Date of Publication:** 25-04-2025

ABSTRACT

In an increasingly interconnected digital world, cybercrime has emerged as a transnational threat demanding coordinated global responses. India, as one of the largest digital economies, plays a pivotal role in fostering international cooperation to combat cybercrime. This study explores India's engagement in global cybersecurity initiatives, focusing on its bilateral and multilateral collaborations, legislative frameworks, and partnerships with international organizations such as INTERPOL, UNODC, and the Global Forum on Cyber Expertise. The paper highlights India's efforts to harmonize cyber laws, participate in information-sharing networks, and contribute to cross-border investigations. It also addresses the challenges India faces, including jurisdictional issues, data sovereignty concerns, and evolving cyber threats. By analyzing India's proactive strategies and policy reforms, the study underscores the nation's commitment to enhancing global cybersecurity and shaping a cooperative, resilient digital ecosystem.

Keywords- Cybersecurity, Cybercrime, International Cooperation, Digital Policy.

I. INTRODUCTION

The internet has revolutionized human interactions, business, and governance, creating global connectivity alongside new vulnerabilities to cybercrime, including data theft and ransomware. As cyber threats are inherently transnational collaboration is essential. India, with its growing digital economy, faces significant cyber challenges, from data breaches to attacks on critical infrastructure. This paper examines the role of international cooperation in combining cybercrime, focusing on India's contributions, legal frameworks, and case studies and case studies, while comparing its approach to other nations to provide a comprehensive analysis of its role in global cybersecurity.

Cybercrime includes various illegal activities conducted through digital devices and the internet, such as hacking, identity theft, financial fraud, and ransomware attacks. Its global nature complicates law enforcement, as criminals can operate from one country while targeting victims in another. National borders are irrelevant in cyberspace, making it hard for individual countries to investigate and prosecute cybercriminals effectively. This highlights the need for international cooperation, where countries can collaborate through agreements to create a coordinated response to combat cybercrime.

Figure 1: Verticals of I4C

Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)

Stallion Journal for Multidisciplinary Associated Research Studies
ISSN (Online): 2583-3340
Volume-4 Issue-2 || April 2025 || PP. 315-319 https://doi.org/10.55544/sjmars.4.2.21

1.1 Forms of International Cooperation

- MUTUAL LEGAL ASSISTANCE (MLATs): Countries use MLATs to share evidence and legal documents for cross-border investigations, but these processes can be slow, delaying law enforcement.
- JOINT CYBERCRIME INVESTIGATIONS: Law enforcement agencies from different nations collaborate to investigate cybercrimes that span multiple jurisdictions.
- CAPACITY BUILDING AND TECHNICAL ASSISTANCE: Developed countries help less developed nations by providing training and resources to strengthen their ability to combat cybercrime.
- HARMONIZATION OF CYBERCRIMES LAWS: Efforts like the Budapest convention aim to standardize cybercrime laws worldwide, making it easier for countries to work together in investigations and prosecutions.

1.2 India's Legal Framework for Combating Cybercrime

- India's approach to cybercrime is primarily governed by the Information Technology Act, 2000 (IT Act), which was updated to address new cyber threats. Key updates in the 2008 Amendment include:
- SECTION 66: Criminalizes hacking, with penalties of up to three years in prison and fines.
- SECTION 66C: Addresses identity theft, penalizing the fraudulent use of someone else's electronic credentials.
- SECTION 66F: Covers cyberterrorism, with severe penalties, including life imprisonment for threats to national security.
- SECTION 67: Regulates the publication of obscene content online.
- In addition to the IT Act, the Digital Personal Data Protection Act (DPDP Act), 2023 was introduced to protect individual privacy and regulate personal data handling. This Act aligns with global standards like the GDPR and gives individuals the right to access, correct, and delete their data, while imposing obligations on businesses for data protection. Overall, these laws represent a significant step in enhancing India's cybersecurity and privacy framework.

1.3 Challenges faced by India's Cyber law

Lack of Comprehensive Data Protection: Without a dedicated data protection law, India struggles to safeguard personal data compared to countries with stricter regulations, like those in the EU.

Cybercrime Underreporting: Many cybercrimes go unreported due to victims' lack of awareness or concerns about law enforcement's ability to handle digital crimes effectively.

Enforcement and Implementation: Although the IT Act provides a strong legal framework, challenges in enforcement arise from limited resources, a lack of technical expertise among law enforcement, and complex jurisdictions issues.

II. METHODOLOGY

This research paper is using the literature survey-based methodology to explore the objectives based on research topic. In recent years, the exponential rise in cybercrime has necessitated robust international cooperation, with India playing an increasingly significant role in the global cybersecurity landscape. The country has been actively engaging in bilateral and multilateral dialogues to enhance collective cyber defense capabilities. For instance, the Sixth India–UK Cyber Dialogue [7] and cybersecurity collaborations with the United States [8] highlight India's commitment to transnational coordination in combating cyber threats. These partnerships aim not only to facilitate real-time information exchange but also to standardize legal frameworks for effective cross-border prosecution.

India's national cybersecurity strategies have been instrumental in shaping its global digital diplomacy. Scholarly work has analyzed India's evolving role in international forums and agreements, asserting that its cybersecurity diplomacy is moving towards building strong, rules-based global alliances [1], [10], [11]. The establishment of institutions like the Indian Cyber Crime Coordination Centre (I4C) [8] and participation in multinational cyber exercises such as 'Synergy' [9] underscore India's proactive stance in international cybersecurity preparedness.

A comparative lens reveals that India's strategy mirrors global best practices while retaining a unique focus on sovereignty and national interest. A study comparing cybersecurity policies across nations places India's framework within the broader global discourse [12], highlighting strengths in legal readiness but also identifying gaps in cyber incident response capacities. At the same time, real-world developments like the surge in organized cyber scams from India [6] reflect the urgency for capacity-building and international law enforcement collaboration.

Academic literature also addresses India's domestic readiness to tackle cybercrime. Legal studies point to ongoing reforms in cyber law enforcement and procedural justice systems aimed at aligning with global cyber norms [2], [3]. Additionally, scholars emphasize the challenges faced by Indian law enforcement in detecting, investigating, and prosecuting cyber offenses that originate across multiple jurisdictions [4], [5].

Cyberwarfare and geopolitical cyber tensions have also been a growing concern, especially in the South Asian context. Researchers note the strategic implications of India's cyber stance, particularly with regional adversaries, and advocate for stronger cyber defense infrastructure integrated with global threat intelligence systems [4]. This has prompted a shift in defense policy, where cyber resilience is becoming as critical as traditional military readiness [1], [13].

Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)

Stallion Journal for Multidisciplinary Associated Research Studies
ISSN (Online): 2583-3340
Volume-4 Issue-2 || April 2025 || PP. 315-319 https://doi.org/10.55544/sjmars.4.2.21

Further, the impact of global disruptions like the COVID-19 pandemic has tested the resilience of India's cybersecurity systems. Analysis of cyber-attacks during the pandemic suggests that India, like many nations, witnessed a surge in cyber intrusions targeting healthcare and government sectors [14]. These events highlight the importance of international cooperation not just for reactive strategies but also for proactive threat intelligence sharing and infrastructural fortification.

Foundational texts in cyber criminology offer a theoretical basis for understanding the evolving nature of cybercrime in India and reinforce the importance of international law, behavioral profiling, and predictive modeling [15]. When contextualized within India's socio-legal ecosystem, these theories support the country's ongoing efforts to harmonize domestic laws with international conventions.

III. ANALYSING ROLE OF INDIA IN GLOBAL CONTEXT

In an era defined by rapid digitalization and increasing cyber threats, cybercrime has transcended national borders, necessitating robust international collaboration. India, as a major digital hub and emerging global power, has significantly intensified its role in combating cybercrime through international cooperation.

3.1 India's Role in International Cooperation on Cybercrime

As one of the largest digital economies globally, India acknowledges the need for international cooperation to combat cybercrime. While it is not a signatory to the Budapest Convention on Cybercrime, India actively engages in various international cybersecurity initiatives to enhance collaboration and address cyber threats effectively are as following:

Bilateral and Multilateral Agreements: India-United States Cyber Framework: India and the U.S. have enhanced cybersecurity cooperation through an agreement focused on information sharing, critical infrastructure protection, also addressing cybercrime and terrorism in the Homeland Security Dialogue.

India-European Union Cyber Dialogue: India regularly engages with the EU in discussions on data protection, cyber resilience, and combatting cybercrime. Despite not signing the Budapest Convention, India collaborates with EU countries on cybersecurity matters.

Shanghai Cooperation Organization (SCO): As a member of the SCO, India addresses cybersecurity issues, particularly in countering cyberterrorism and protecting critical infrastructure.

3.2 India's Global Cybersecurity Index (GCI) Performance:

India has been recognized as a Tier 1 country in the 2024 Global Cybersecurity Index (GCI), published by the International Telecommunication Union (ITU). This ranking highlight India's commitment to enhancing its cybersecurity across five key areas: legal measures, technical measures, organizational measures, capacity building, and cooperation. Notably, India has excelled in the legal and organizational pillars, largely due to the IT Act and the establishment of the Indian Computer Emergency Response Team (CERT).

3.3 Comparative Analysis: India and Other Nations

India vs. United States: The U.S. has a strong data protection practices but lacks a single comprehensive law like the EU's GDPR. India has introduced the Digital Personal Data Protection Act (DPDP Act) in 2023, which mirrors some GDPR principles, such as requiring consent for data collection and allowing rights to correction and erasure. However, differences remain, particularly in enforcement and data localization, which may hinder full alignment with global standards.

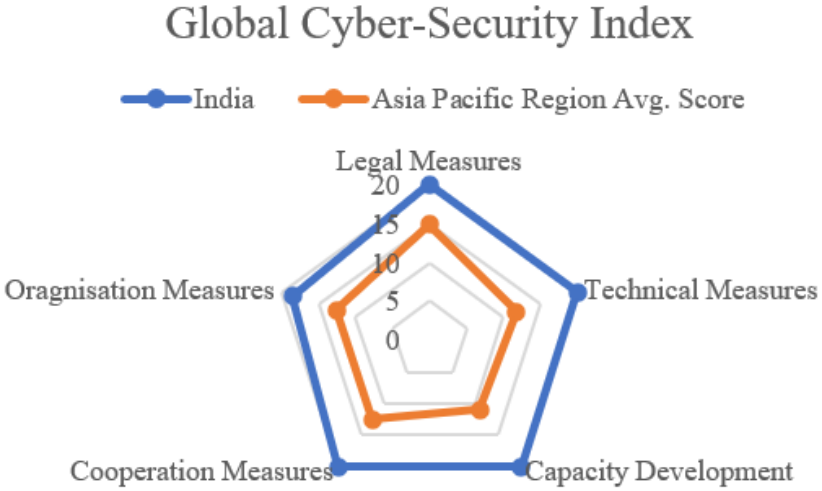

Figure 2. Global Cyber-Security Index

Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)

Stallion Journal for Multidisciplinary Associated Research Studies
ISSN (Online): 2583-3340
Volume-4 Issue-2 || April 2025 || PP. 315-319 https://doi.org/10.55544/sjmars.4.2.21

India vs. European Union: The EU is known for its robust data protection through the GDPR, setting high standards globally. India previously lacked a comprehensive data protection law, but the new DPDP Act moves it closer to GDPR standards. However, without equivalent domestic legislation, Indian companies may struggle to comply with EU regulations when doing business.

India vs. China: China's cybersecurity approach is marked by strict government control and regulations like its Cybersecurity Law, which enforces data localization and surveillance. In contrast, India's cybersecurity is more decentralized and emphasizes individual rights. However, India faces challenges in effectively enforcing its laws due to limited resources and technical expertise.

3.4 Legal Case Studies in Cybercrime from Indian Jurisdiction:

Shreya Singhal v. Union of India (2015) this landmark case resulted in the Supreme Court striking down Section 66A of the IT Act, which criminalized sending "offensive" messages online. The Court found it unconstitutional as it violated the right to freedom of speech under Article 19(1) (a) of the Constitution. The ruling highlighted the need for clear cybercrime laws to protect civil liberties.

Suhas Katti v. State of Tamil Nadu (2004) this case marked one of the first convictions under Section 67 of the IT Act, which addresses the transmission of obscene material. A man was convicted for posting defamatory messages about a woman in a Yahoo group. He was sentenced to imprisonment and fines, setting a precedent for handling cyber harassment and defamation in India.

Kamlesh Vaswani v. Union of India (2014) in this case, the Supreme Court examined online pornography, especially child pornography. The petitioner sought a ban on websites hosting such content. While the Court acknowledged the need for regulation, it also emphasized the challenge of balancing censorship with freedom of speech, leading to discussions on the role of intermediaries like ISPs in preventing illegal content.

IV. CHALLENGES AND OPPORTUNITIES IN CROSS-BORDER CYBERCRIME COOPERATION

With the increasing global interconnectivity of digital systems, cybercrime has become a significant transnational threat. For India, a rapidly digitizing economy and a key geopolitical player, cross-border cooperation in combating cybercrime is both a necessity and a challenge.

4.1 Challenges:

- Implementation and Enforcement: The DPDP Act (2023) modernizes data protection, but enforcing compliance, especially among small businesses, remains a challenge.
- Cybercrime Underreporting: Many cybercrimes go unreported due to victims' lack of awareness or mistrust in law enforcement's ability to handle these issues.
- Capacity Building: Law enforcement and judicial bodies require improved technical skills to effectively investigate and prosecute cybercrimes.

4.2 Opportunity:

- Strengthening International Partnerships: India can enhance collaboration with countries like the U.S., U.K., and Japan in areas like information sharing and joint investigations.
- Adopting International Standards: Enacting comprehensive laws, like the Personal Data Protection Bill, can improve India's global standing and cooperation with countries that have strict data protection standards.
- Technological Investments: Investing in advanced cybersecurity technologies and establishing specialized cybercrime units can boost India's capacity to address cyber threats.

A key opportunity for India in combating cybercrime is the Digital Personal Data Protection Act (DPDP Act), 2023. This Act includes provisions for cross-border data transfers, enhancing cooperation with countries like those in the European Union that have strict data protection regulations. By aligning with international best practices, India can strengthen partnerships with global law enforcement and improve its participation in international investigations and joint operations against cybercrime.

V. CONCLUSION

India has made notable progress in combating cybercrime with new data protection laws and enhanced cybersecurity frameworks. However, challenges such as enforcement gaps, underreporting of cybercrimes, and the need for technological investment remain. As India rises in the Global Cybersecurity Index (GCI), it must strengthen law enforcement capacity and align its laws with international standards. Positioned strategically in the Asia-Pacific, India can foster global collaboration in cybercrime efforts. In summary, while advancements have been made, addressing these challenges will be crucial for India to shape future international efforts against cybercrime.

Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)

REFERENCES

[1] Y. Fernandes and N. Abosata, "Analysing India's Cyber Warfare Readiness and Developing a Defence Strategy," *arXiv preprint*, Jun. 2024, arXiv:2406.12568.
[2] K. Rani, "Cybercrime and Legal Responses in the Indian Jurisdiction," *Indian Journal of Law*, vol. 1, no. 1, pp. 35–41, Nov. 2023, doi: 10.36676/ijl.2023-v1i1-05.
[3] N. Neethu, "Role of International Organisations in Prevention of Cyber-Crimes: An Analysis," *Tech. Rep.*, National Academy of Legal Studies and Research, Dec. 2020, doi: 10.13140/RG.2.2.21906.63685.
[4] G. Mustafa, Z. Murtaza, and K. Murtaza, "Cyber Warfare between Pakistan and India: Implications for the Region," *Pakistan Languages and Humanities Review*, vol. [Online], no. 4-I2, pp. 59–71, 2020, doi: 10.47205/plhr.2020(4-I)2.5.
[5] S. Rani *et al.*, "Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey," *arXiv preprint*, Oct. 2020, arXiv:2010.08793.
[6] "India's Cyber-Scam Epidemic is Part of a Multibillion Global Industry," Scroll, Jan. 31, 2025. [Online]. Available: Reddit: r/india.
[7] "Sixth India–UK Cyber Dialogue," Press Release, Ministry of External Affairs, Gov't of India, Jul. 3, 2024. [Online]. Available: Reddit: r/GeopoliticsIndia.
[8] "Indian Cyber Crime Coordination Centre (I4C) Inauguration & India–US MoU," Press Information Bureau, Jan. 10, 2020; *The Hindu*, Jan. 18, 2025. [Online].
[9] "CERT-In Hosts Cyber Exercise 'Synergy' with 13 Countries," Ministry of Electronics & IT, Sept. 2022. [Online].
[10] "India's Cybersecurity Diplomacy: Building Global Alliances," *Research Report*, 2024. [Online].
[11] P. K. Chaudhary, "India's cybersecurity diplomacy: Building global alliances," *ShodhKosh J. Visual Perform. Arts*, vol. 4, no. 2, pp. 2199–2203, Dec. 2023, doi: 10.29121/shodhkosh.v4.i2.2023.3386.
[12] A. T. Odebade and E. Benkhelifa, "A Comparative Study of National Cyber Security Strategies of Ten Nations," *arXiv preprint*, Mar. 2023, arXiv:2303.13938.
[13] M. Chaturvedi, A. Unal, P. Aggarwal, S. Bahl, and S. Malik, "International cooperation in cyberspace to combat cyber crime and terrorism," in *Proc. IEEE 21st Century Norbert Wiener Conf.*, 2014, pp. 102–114, doi: 10.1109/NORBERT.2014.6893915.
[14] H. S. Lallie *et al.*, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," *arXiv preprint*, Jun. 2020, arXiv:2006.11929.
[15] S. Jaishankar, *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, CRC Press, 2011; cited contextually for foundational theory in cybercrime studies in India.

Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)