© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718726

AI And Cybersecurity – An Indian and Bangladeshi Cyber-Border Perspective

KRUSHNA BHAMRAY PATIL
Political Science Department, Savitribai Phule Pune University.

Abstract- ***As globalization gears up every decade, the blurred borders are enhancing geo-political and economic inclusivity on one hand but on the other are causing significant and potentially severe security implications. Among these, Cybercrimes since the past two and a half decades have increased exponentially resulting in fueling political, social and economic instability. The increase in cyber threats and attacks has prompted many countries to collaborate in addressing this shared challenge. Similarly, in the south Asia block - India and Bangladesh formalized an MOU on joint cybersecurity cooperation in 2017 to facilitate and enhance bilateral cooperation to tackle the issue related to cyber-threats. This research paper navigates the loopholes with respect to framework and implementations of the MOU under India's CERT-In and Bangladesh's BGD e-Gov CIRT and how it can be made more effective and reliable in dealing with cyber-border security.***

Keywords - India, Bangladesh, BGD e-Gov CIRT, CERT-In, Cyber-crimes, Cybersecurity, BGD e-Gov CIRT, India, National Security, South-Asia.

I. INTRODUCTION

The MOU signed on cybersecurity in 2017 acted as a testament to proliferating ties between nations that not only share borders but also happen to share historic, cultural and economic ties. India and Bangladesh have had prosperous relations with both the countries being active in formulating and maintaining bi-lateral cooperations spanning from energy sector to disaster management. Both the nations have been active in fulfilling their respective national interest which collectively resulted into establishing proactive relations on one hand and collective development of the India-Bangladesh geo-political area.

The relations between the two nations have been ever developing and have been directed in tackling the issues of the current times. On this account, the past two and a half decades have witnessed an increase in issues related to cybercrimes and have brought the neighboring countries together to form collective preventive measures that can be transparent, reliable, and efficient.

Cybercrime in India marked decisive escalation in 2017, as reflected in the National Crime Bureau NCRB data. A total of 21, 796 cybercrimes cases were recorded that year, representing a sharp 77% increase over 2016. This surge was nearly quantitative but also structural.

As the expansion was largely attributed to the introduction of new crime categories, including cyber blackmailing, cyber stalking, and fake news-related offenses. The revised classification framework significantly broadened the scope of reporting, thereby revealing the growing scale and complexity of cyber-enabled crimes within the stand at approximately 6%.

This rising trend coincided with significant systematic vulnerability - a 2015 Kaspersky Security Bulletin reported that 69.55% of unique users in Bangladesh were exposed to local viral infections plain the country the most affected globally at that time. These risks are underscored by major pre-2017 incidents, most notably the US $101 million Bangladesh Bank cyber heist in February 2016 and coordinated attacks on multiple bank ATM booths, highlighting both the scale and sophistication of cyber threats facing the country.

Hence, these trends collectively underscored an alarming need of the hour to craft a dedicated and forward-looking Memorandum of Understanding (MOU), Aimed at strengthening bilateral cyber cooperations, enhancing information-sharing mechanisms, and developing coordinated prevention and response frameworks to effectively address the

rapidly evolving and transnational nature of cyber threats.

Accordingly, an MOU was formalized in 2017 between India's Computer Emergency Response Team (CERT-In) under the Ministry of Electronics and Information Technology and Bangladesh's e-Government Computer Incident Response Team (BGD e-GOV CIRT) under Ministry of Posts, Telecommunication and Information Technology by setting up a joint committee in cyber security.

The objective of formalizing this MOU was to point out the need for greater collaboration to share knowledge and expertise in exercise on cyber resilience, network vulnerability, cyber assessment, and awareness.

Following this, the 7th round of India-Bangladesh Joint Consultative Commission was formed in 2022 to work closely and deepen cooperation in the areas of IT and cybersecurity, renewable energy, agriculture and food security; etc. This collaborative momentum was further reinforced at the regional level through multilateral mechanisms such as Bay of Bengal Initiative for Multisectoral Technical and Economic Cooperation, held in New Delhi in 2022, reviewed and updated the draft Five-Year Action Plan for BIMSTEC Cybercrime Cooperation Framework among law enforcement agencies.

But, despite all these active measures taken up by both the countries the MoU suffers from considerable technical loopholes which is not allowing it to fulfill the promises and efforts that have been put into it to foster a healthy cyber-border security framework.

Despite the presence of formal cybersecurity laws and bilateral initiatives, the cybersecurity frameworks in both India and Bangladesh continue to lack conceptual and operational clarity, leading to fragmented implementation and enforcement. Several key stakeholders, including private sector actors, transnational digital service providers, and non-state entities, remain largely outside the effective ambit of existing cybersecurity policies, thereby limiting their overall effectiveness.

Furthermore, the present legal framework focuses on predominantly on addressing cybercrimes originating within national borders, offering inadequate responses to cross-border cyber threats, and the 2017 India-Bangladesh Memorandum of Understanding on cybersecurity cooperation, although ambitious in its objectives, has so far fallen short of delivering meaningful and effective joint cyber protection.

II. THE MEMORANDUM OF UNDERSTANDING SIGNED BETWEEN INDIA AND BANGLADESH

Rapid digitization across the South Asia region has significantly contributed to economic growth across the primary, secondary, and tertiary sectors. However, this digital transformation has simultaneously rendered the region increasingly vulnerable to cyber threats including online frauds, identity threats, doxing, and sophisticated cyber intrusions. These emerging threats pose substantial risks to national security and state sovereignty, particularly in countries with expanding digital ecosystems.

In response to the escalating cyber threats landscape over the past two decades, India and Bangladesh formalized an MOU to jointly address cybercrimes and enhance cybersecurity cooperation. This MoU represents a pioneering bilateral initiative in South Asia. Aimed at institutionalizing collaborations against cyber threats. Moreover, it reflects India’s broader strategic efforts to operationalize its act east policy by strengthening regional partnership in non-traditional security domains such as cyberspace.

This research paper identifies a critical research gap centered on Article 5 of the Memorandum of Understanding (MoU), which stipulates that all cooperative activities taken under article 2,3 and 4 relating the scope of cooperation, implementation, mechanisms, and joint committee shall be conducted in accordance with the applicable rules, laws and regulations of each country. Though this provision respects national sovereignty, it implicitly places the responsibility of addressing cybersecurity threats on individual domestic legal and regulatory frameworks rather than on a harmonized or collective regime. As a result, cybersecurity cooperation is operationalized

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718726

through a parallel national approach rather than an integrated bilateral mechanism.

The study argues that this structural limitation undermines the core objectives of the MoU. In the absence of a unified or interoperable cybersecurity framework, divergences in the legal, institutional and regulatory architectures of India and Bangladesh constrain effective cooperation.

These disparities complicate joint implementation, information sharing and coordinated responses to transnational cyber threats, consequently, despite the formal existence of the MoU, both countries continue to experience a rise in cybercrime affecting key economic sectors. This highlights the need for a greater regulatory alignment of the development of common operational standards to ensure that bilateral cybersecurity cooperation translates into tangible and effective outcomes.

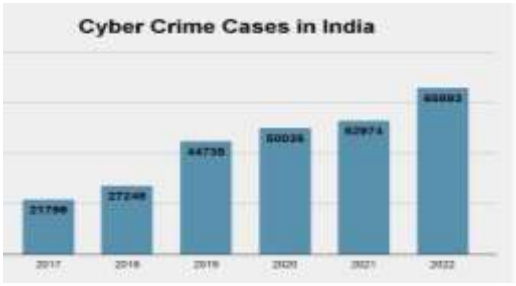
This argument can be substantiated by the rise of cyber threats faced by both the countries post 2017, after the formulation of the MoU.

III. CYBER CRIMES IN INDIA POST 2017

Cybercrimes in India have witnessed a sustained and sharp increase, reflecting the evolving tactics employed by offenders to exploit digital platforms. According to the crimes in India report 2022 published by the national crime record bureau, a total of 65,893 cybercrimes cases registered during 2022, marking a 24.4% rise over 2021, when 52,974 cases were reported.

Correspondingly, the cybercrime rate increased from 3.9% in 2021 to 4.8% in 2022, indicating a widening exposure of the population to digital threats. Fraud emerged as the dominant motive, accounting for 64.8% of all registered cases - 42.710 incidents, followed by extortion at 5.5% - 3,648 cases and sexual exploitation at 5.2% - 4,343 cases. Notably 2022 recorded the highest number of cybercrime cases in India to date, underscoring the scale and complexity of the challenge. This upward trend intensified further in 2023, when registered cybercrime cases surged to 86,420, marking a 31.2% increase compared to 2022.

This situation escalated rapidly in 2024, as reports from the national cybercrime reporting portal indicated a 42.08% rise in reported incidents, reaching approximately 22.68 lakh cases, accompanied by a dramatic 206% increase in financial losses. Despite this surge criminal justice response remains constrained, as reflected in a low charge sheeting rate of only 29.6% highlighting persistent gaps in investigation, prosecution capacity and institutional preparedness to effectively address cyber-enabled offenses.



Source: National Crime Bureau, graph indicating rise of cybercrimes in India post 2017.

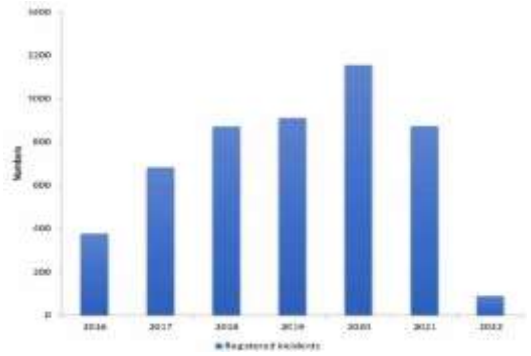
IV. CYBER CRIMES IN BANGLADESH POST 2017

Post 2017 studies indicate that nearly 52% of banks remain at high cyber risks, with institutions facing between 145 and 638 cyberstalk attempts daily during 2023-2024, underscoring persistent systemic weakness. Financial fraud has expanded alongside digital commerce, with e-commerce - related offences accounting for 14.64% of reported cybercrimes by 2022.

notably, 72% of online banking frauds exploited the SWIFT system, while a further 20% targeted internal banking software, social media platforms have emerged as a dominant vector for cybercrimes as reflected in Dhaka metropolitan police data for 2023 where 23.89% cases involved Facebook breaches, online extortion or fraud. Cyber risks are further compounded by gender - based vulnerabilities with studies suggesting that approximately 73% of Bangladeshi women have experienced cybercrimes in the form of harassing, stalking or non-consensual dissemination of images.

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718726

Technological threats have also intensified as malware and ransomware incidents increased by 71.39% according to BGD e-GIV CIRT, primarily due to the continued use of outdated and insecure systems. Although cumulative banking sector IT investment reached BDT 534.13 billion between 2000-2024, only about 5% was allocated to dedicated cybersecurity measures, leaving financial institutions inadequately prepared to prevent, detect and respond to evolving cyber threats



Source: SAIla Rapti, Nabila Fahria, Sunita Rani Das."Role of Bangladesh Bank on Cybersecurity in FinTech". book-Cross-Industry Applications of Cyber Security, p.71-90.

Framework related deficiencies within the India-Bangladesh cybersecurity MoU substantially constrains its operational effectiveness because the agreement is designed primarily as a cooperative instrument rather than a binding regulatory framework. The MoU emphasises information exchange, capacity building and mutual assistance, but implementation is explicitly subject to the respective domestic laws, rules and institutional capabilities if each country.

This reliance on divergent national legal regimes where India possesses a relatively more structured policy architecture while Bangladesh lacks comprehensive standalone data-protection statutes creates asymmetry in obligation, enforcements capacity and response timelines. In the absence of harmonized legal standards, uniform standards, uniform incident reporting protocols, or enforceable compliance mechanisms, cross-border cyber incidents cannot be addressed through streamlined procedures.

Instead, coordination becomes coordination becomes contingent on voluntary cooperation, which may delay intelligence sharing, hinder joint attribution efforts, and weaken the deterrent effect that a more integrated legal framework could provide.

Institutional design limitations within the MoU further exacerbates its efficiency. Although the agreement involves collaborations between the national computer emergency response team and establishing a joint committee for implementation.

The framework largely restricts cooperation to technical consultations, training and best practices of exchanges rather than creating a robust, multi-layered governance structure with clearly defined authority and accountability. The absence of strong oversight provisions, dispute resolution mechanisms and operational leadership capable of directing coordinated investigations across jurisdiction results in fragmented execution.

Moreover, the framework does not sufficiently integrate law-enforcement agencies, judicial institutions, or private-sector stakeholders into a structured compliance architecture, thereby limiting its ability to translate strategic intent into rapid, rights-sensitive enforcement. Consequently, while the MoU represents an important diplomatic initiative, its current institutional and procedural design constraints, timely decision-making, effective crisis response, and sustained cross border cybersecurity coordination.

India's framework largely is centered on the Information Technology Act, 2000 and policy instruments such as National Cyber Security Policy 2013 and the National Cyber Security Strategy 2020, remains fragmented and a reactive offering limited coverage for contemporary threats like ransomware, deepfakes and AI-enabled attacks. Bangladesh's cyber security act, while more recent, reflects its own structural weaknesses such as vague qualification standards, leadership and forensic personnel, excessive centralization in decision making bodies, low or inconsistent penalties, unclear corporate liabilities and protracted investigation timelines.

This normative misalignment complicates mutual assistance, evidence sharing and joint operations envisioned by the MoU, as conduct criminalized or prioritized in one jurisdiction may be ambiguously regulated or weekly sanctioned in the other.

Another loophole can be highlighted as gaps in public-private collaborations and critical infrastructure protection. In India, mandates for cybersecurity audits and incident reporting remain largely sector-specific, notably the banking sector, leaving healthcare, SMEs and other critical services with uneven compliance incentives.

In Bangladesh, enforcement capacity and oversight clarity pose parallel challenges. Although both countries rhetorically endorse public-private partnerships, operational mechanisms for mandatory breach of reporting, coordinated response, and shared threat intelligence are under-developed. Without binding sector-specific standards, empowered infrastructure protection authorities, and asynchronous compliance regimes, the MoU's applicability and effectiveness remain aspirational.

Against the backdrop of evolving regulatory quality, fragmented institutional mechanisms and persistent challenges in cybersecurity and AI governance in Bangladesh and India, effectiveness of coordination instruments such as MoU assumes critical importance. While the MoU have traditionally served as foundational tools for cooperation between government, agencies and international partners, their impact has often remained limited due to vague commitments, weak monitoring mechanisms and the absence of enforceable accountability frameworks.

As governments increasingly integrate artificial intelligence into public administration and policy implementation, AI represents a transformative opportunity to reimagine MoU’s as dynamic, outcome-oriented governance instruments rather than static declarations of intent. By embedding AI enabled tools for data-driven planning, real-time monitoring, compliance assessment, and risk anticipation, MoU’s can be aligned more closely with cybersecurity imperatives, regulatory quality, and institutional trust. In this

V. AI AND THE FUTURE OF THE MOU

Artificial intelligence has emerged as a transformative force in the domain of cybersecurity, fundamentally reshaping how cyber threats are detected, analyzed, and mitigated.

As governments and organizations increasingly rely on digital infrastructure and data-intensive AI systems, the scale, speed and sophistication of cyberattacks have grown correspondingly, rendering conventional rule-based security mechanisms insufficient.

In this context, AI driven cybersecurity solutions leverage machine learning mechanisms and big data analytics to process vast volumes of systems logs, network traffic and user behavior in real time, enabling the early identification of anomalies that may signal cyber threats.

Unlike static security frameworks, AI systems possess adaptive learning capabilities allowing them to evolve in response to emerging and previously unseen attack vectors. Empirical studies reveal that AI is predominantly applied in threat detection, where algorithms assess behavioral patterns, identify malicious activities such as brute-force login attempts, and recognize deviation indicative of cyber instructions. Moreover, by analyzing historical attack data and recurring threat patterns, AI systems can anticipate potential vulnerabilities and support predictive risk management.

Beyond detection and plays a critical role in automating cyber-incident responses, thereby enhancing the speed, efficiency and reliability of cybersecurity defenses. This growing integration of AI into cybersecurity underscores as a foundational pillar of AI readiness and secure digital governance.

VI. HOW CAN AI MAKE THE MOU EFFECTIVE?

AI can serve as a critical unifying mechanism for harmonizing cybercrimes laws, regulatory practices, and enforcement cooperation between India and Bangladesh, particularly in the light of transnational and increasingly AI-enabled nature of cyber threats.

AI can facilitate comparative legal analytics that can comparatively examine cyber laws, enforcement outcomes, judicial interpretation and regulatory gaps in both jurisdiction allowing policymakers to identify the areas of convergence and divergence with empirical precision.

AI can be used to address the issue related to the framework of the mou by enabling evidence-based design, implementation and evaluation of mou obligation. Through machine learning and advanced analytics, AI systems can assess historical cyber incident data, institutional performance records, and compliance trends to inform realistic targets, role allocations, and timelines during the drafting stage of the MoU.

Natural language processing tools can further improve legal clarity by identifying ambiguities, overlaps and inconsistencies in mou text, ensuring alignment with domestic cybersecurity laws and international norms. During implementation, AI enabled dashboards to facilitate real time monitoring of joint commitment such as information sharing, capacity building, or incident response by tracking predefined indicators and flagging deviations.

in this way, AI strengthens transparency, accountability and trust among signatory parties, thereby enhancing the credibility and enforceability of mou in the cybersecurity domain.

VII. AI AS UNIFYING MECHANISMS FOR COMMON CYBER CRIME LAW BETWEEN INDIA AND BANGLADESH

AI also holds substantial potential as a unifying instrument for harmonizing cybersecurity laws and cybercrimes responses between India and Bangladesh. Despite shared digital ecosystems and cross border cyberthreats, differences in legal definitions, enforcement procedures, and institutional capacities often hinder effective cooperation.

AI driven comparative legal analytics can assist policymakers in identifying legal standards without undermining sovereignty. Common AI-based threat classification systems, digital evidence-based analysis tools, and incident reporting frameworks can further support mutual legal assistance and coordinated investigations. by embedding AI governance principles such as transparency, accountability and data protection into bilateral MoU's. Both countries can move towards a shared normative framework for addressing cybercrimes.

AI can facilitate such convergence by enabling functional and operational harmonization of cybercrime governance without requiring an identical legal system.

AI driven comparative legal analytics can systematically examine cyber laws, enforcement outcomes, judicial interpretations, and regulatory gaps in both jurisdictions, allowing policymakers to identify areas of convergence and divergence with empirical precision. This approach is particularly valuable given that Bangladesh still underperforms in AI-related R&D investment - spending less than 0.03% of GDP - and scored 0.38 on the imfs AI preparedness index, compared to India's 0.49.

embedding AI-assisted legal mapping within bilateral mou would allow both states to formulate interoperable definitions of cyber offences, shared evidently standards, and mutually recognizable enforcement thresholds, thereby strengthening mutual legal assistance and reducing jurisdictional friction in cross-border cybercrime investigations.

Operationally, AI can standardize cybercrimes detection, attribution and response mechanisms across India and Bangladesh through shared technical benchmarks. Common AI-based threat classification systems, digital forensic tools, and predictive risks models can enable CERT's financial regulators, and law enforcement agencies on both sides of the border to interpret cyber incidents using aligned criteria. This is particularly relevant for financial fraud, phishing, ransom wear, and AI generated cybercrimes-areas where Indian banks have already reported up to 40% reduction in successful phishing attacks following AI adoption, while Bangladesh continues to lack real-time AI driven threat detection capabilities.

AI powered digital evidence analysis can also strengthen prosecutorial cooperation by preserving

chAIn-of-custody, improving attribution accuracy, and enhancing evidentiary long-standing obstacles to cross-border cybercrime prosecution.

From a strategic perspective, AI can also underpin the development of shared governance principles and regional cyber norms between India and Bangladesh.

Joint AI oversight mechanisms such as cross-border audits, explainable AI based decision systems, and shared threat intelligence platforms can promote common standards of transparency, accountability, and data protection. International experience offers a compelling benchmark: following the 2007 cyberattacks, Estonia institutionalized AI-enabled cyber defense strategies and established the NATO Cooperative Cyber Defense Center of Excellence demonstrating how technological integration and legal coordination can reinforce national and regional cyber resilience.

By embedding similar AI enabled mechanisms within bilateral MoU's, India and Bangladesh can gradually carve out a shared normative and operational framework for tackling cybercrimes, one that balances sovereignty with cooperation and innovation with legal certainty.

In this sense, AI functions not merely as a technical tool but as a regulatory bridge, enabling legal convergence, institutional trust, and sustained bilateral cooperation in an increasingly hostile cyber domain.

VIII. FUTURE TRAJECTORY OF THE INDIA-BANGLADESH MOU IN THE AGE OF ARTIFICIAL INTELLIGENCE

The future effectiveness of the memorandum of understanding between India and Bangladesh will depend on how flexibly and innovatively article 5 is operationalized in response to the evolving nature of cyber threats. While Article 5 mandates that cooperative activities under article 2,3 and 4 be carried out in accordance with domestic laws and regulations, this study demonstrates that such a parallel national approach is increasingly inadequate for addressing transnational, AI enabled cybercrime.

The trajectory of the mou must therefore shift from procedural cooperation to functional interoperability, where outcomes are jointly produced even as legal sovereignty is preserved. Artificial intelligence provides a viable pathway for this transition by enabling technical and operational convergence without formal legal harmonization. Through AI-driven threat intelligence platforms, automated anomaly detection systems, and predictive risk analytics, both countries can synchronize their cybersecurity responses in real time.

Embedding such mechanisms within the mou through technical annexes or joint implementation protocols would allow cooperation to move beyond ad hoc information sharing towards continuous, machine-supported coordination. This approach also offers a practical means of addressing institutional asymmetries, particularly Bangladesh's comparatively limited AI readiness and cybersecurity capacity, by enabling shared situational awareness and collective response mechanisms.

International experience reinforces the feasibility of this trajectory. Singapore demonstrates how exercise-based AI integration institutionalizes cyber preparedness, while European Union agency for cybersecurity (ENISA) provides a model for layered AI governance that balances operational effectiveness with regulatory accountability.

Australia further illustrates the importance of securing AI systems themselves through data integrity, model provenance, and early-warning mechanisms. Adapting these practices within the India-Bangladesh MoU framework, such as mandatory joint cyber exercises, explainable AI based evidence standards, and shared notification protocols for AI compromise would significantly enhance the MoU's operational credibility.

Ultimately, the future trajectory of the mou lies in reconceptualizing article 5 as an enabling provision rather than a constraint. By leveraging AI as a bridging mechanism, India and Bangladesh can develop common operational standards, interoperable enforcement practices, and coordinate response architectures that function within domestic legal systems while producing integrated security

outcomes. Such an evolution would transform the mou into a living governance instrument, capable of adapting to the rapidly changing cyber threat landscape.

CONCLUSION

This research has identified a critical gap in the existing India-Bangladesh cybersecurity cooperation framework, centered on the implementation logic of article 5 of the MoU. While the provision appropriately safeguards national sovereignty, its reliance on domestic legal and regulatory frameworks has resulted in a fragmented, parallel approach to cybersecurity governance.

In the absence of a harmonized or interoperable regime, divergences in the legal definitions, institutional capacities and regulatory standards have constrained effective joint implementation, information sharing, and coordinated responses to cross-border cyber threats. The continued rise of cybercrime across key economic sectors in both countries underscores the limitations of the current cooperative model.

The study argues that artificial intelligence offers a strategic solution to this structural constraint by enabling structural alignment. AI enabled tools can enhance real time threat detection, predictive analysis, automated response, and evidence-based decision making, thereby strengthening the practical impact of bilateral cooperation.

When embedded within the MoU framework, AI can help bridge institutional asymmetries, improve trust, and translate diplomatic commitments into measurable cybersecurity outcomes.

In conclusion, the effectiveness of India-Bangladesh MoU in addressing cybercrime will increasingly depend on its ability to integrate AI driven operational mechanisms and learn from international best practices.

Drawing lessons from advanced cybersecurity governance models in Singapore, ENISA and Australia, both countries can reimagine bilateral cooperation as an adaptive, intelligence-driven process rather than a static legal arrangement. Such a shift is essential not only for countering contemporary cyber threats but also for ensuring that the MoU remains relevant, credible, and effective in an era defined by rapid transformations and AI enabled risks.

REFERENCES

[1] PIB. (2025). Curbing Cyber Frauds in Digital India Report (2025). PIB.

[2] TV BRICS. (2023). Experts from Bangladesh and India call for more cyber security training.

[3] Abdullah Al Mamun, Jamaluddin Bin Ibrahim, SK Mamun Mostafa (2021) Cyber Security Awareness in Bangladesh: An Overview of Challenges and Strategies. International Journal of Computer Science and Information Technology Research. Vol. 9, Issue 1, pp:(88-94).

[4] Madhuri Pardesi, P.Jogi Naidu, Goriparthi Naresh (2025) Cybersecurity Laws in India and Beyond: A Comparative Legal Perspective. International Journal of Management and Humanities (IJMH) Volume-12 Issue – 2.

[5] Deepti Lata 1, Dr. Raj Vardhan 2 (2025). An Analytical Study of Cyber Law and Legal Framework in India. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Science (IJIRMPS) Volume 13 Issue 2.

[6] DSCI. (2025). India Cyber Threat Report 2025.

[7] Mohammad Shahadat Hossain, Mahfuza Malika (2025) Cyber Security Governance Under the Cyber Laws of Bangladesh: An Overview. International Journal of Innovative Research and Scientific Studies.

[8] Sohrab Hossain, tasnuva Rashid, Kamrun Nahar, Thahmina Akhter (2023). A study based on the effectiveness of cybersecurity Act 2023 in pursuit of preventing cybercrimes: Bangladesh perspective. International Journal of Law, Policy and Social Review. Volume 6, Issue4, Page No. 22-30.

[9] ImpleVista. Cyber Security Threats: A Growing Concern in Bangladesh.

[10] Md. Robiul Islam, Ayesha Siddika, Nahida Shaulin (2025) AI Readiness and Trust in Government: The Context of Bangladesh and India. In book: Strengthening Human Relations in Organization With AI.

[11] Anoushka Singh (2024) Evaluating the Effectiveness of AI-Powered Cybersecurity Measures in Indian Organizations: A Comparative Study. Indian Journal of Legal Review Volume 4 and Issue 3.

[12] Mohsina Mostafa (2025) Artificial Intelligence and National Security: Can Bangladesh Build Strategic AI Capabilities? BIPSS Commentary.