INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 8 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 8 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-8-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

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

VOLUME 6 AND ISSUE 8 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

AN ANALYTICAL STUDY OF EMERGING CYBERSECURITY TRENDS AND THEIR CHALLENGES IN INDIA

AUTHOR – KARTIK* & DR. POOJA MISHRA**

* STUDENT AT SCHOOL OF LAW, AMITY LAW SCHOOL, AMITY UNIVERSITY, UTTAR PRADESH, INDIA

** PROFESSOR AT SCHOOL OF LAW, AMITY LAW SCHOOL, AMITY UNIVERSITY, UTTAR PRADESH, INDIA

BEST CITATION – KARTIK & DR. POOJA MISHRA, AN ANALYTICAL STUDY OF EMERGING CYBERSECURITY TRENDS AND THEIR CHALLENGES IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (8) OF 2026, PG. 641-651, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I868

ABSTRACT

India's transformation shape the world into a digital economy where governance, banking, healthcare, education and key infrastructure has generated huge digital economy. Regrettably, it has also created a growing and increasingly sophisticated range of cyber-security threats. India, which has over 900 million internet users, largest digital payments infrastructure in the world and a national digitalisation agenda, has both tremendous opportunities and tremendous vulnerabilities in the cyber space. This article provides an analytical overview of the key emerging cyber security trends facing India which include ransomware, state-sponsored advanced persistent threats, artificial intelligence-enabled attacks, vulnerabilities specific to the Internet of Things, cloud security risks, 5G network issues, and cybercrime enabled by cryptocurrency and evaluates the adequacy of India's legal and regulatory apparatus to respond to these trends. India's cybersecurity governance framework based on the Information Technology Act 2000 along with the Digital Personal Data Protection Act 2023 and CERT-In Directions 2022 is essentially inadequate for the contemporary threat environment. This finds its manifestation in definitional obsolescence, institutional fragmentation and enforcement weakness, along with significant regulatory gap for emerging technologies. Following a comparative study of the US, EU and Singapore cyber security frameworks, the article proposes evidence-based reforms including the establishment of a National Cyber Security Act, regulatory sector-specific security standards for critical infrastructure, an IoT security regime, and a sustained investment in the cyber security workforce.

Keywords: Cybersecurity Law; Information Technology Act 2000; CERT-In; Critical Infrastructure Protection; Ransomware; Artificial Intelligence; Internet of Things; 5G Security; Digital Personal Data Protection Act 2023; India.

I. INTRODUCTION

We have now entered an era where digital technology and national security are becoming one of the most important and rapidly evolving areas of law and government. The digital transformation of India, driven by noteworthy policies such as Digital India, Aadhaar-based digital identity infrastructure, Unified Payments Interface, and the progressive digitalisation of government services across various levels, has given rise to a networked digital ecosystem of enormous scale and complexity. India has a little over 900 million Internet users, has the world's largest volume of real-time digital payment transactions and has a fast-evolving digital economy whose scale and sophistication make it one of the most consequential digital ecosystems in the world.

This exceptional digital growth has created great economic and social value. The adoption of

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

VOLUME 6 AND ISSUE 8 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

digital finance has facilitated the acceptance of hundreds of millions from the previously unbanked. Accessible digital government services have contributed to reduced corruption and enhanced service delivery. The outsourcing of information technology and business processes earns annual export revenues worth hundreds of billion dollars. Due to the pandemic, there has been a shift to digital which is also being used in work, education, and healthcare and it has shown the great speed and adaptability that India's digital infrastructure has at a scale that is extraordinary.

Nevertheless, the same digital universe has simultaneously created a threat landscape of unimaginable depth and breadth. It is being exploited daily by an array of malicious actors, ranging from lone hackers and organised transnational cybercrime syndicates to sophisticated state-sponsored advanced persistent threat groups. The perpetration of the latter involves the use of strategic-action-type (or operational) cyber operations on Indian critical infrastructure, defence and government systems. CERT-In, India's Computer Emergency Response Team, reported over 1.3 million cyber security incidents in 2022. The increase in numbers is said to not necessarily indicate that the actual amount of attacks had an increase but rather that there was a growth in actual notification about the attacks. The surge is certainly being attributed to the CERT-In Directions that were issued in April 2022. Cybercrime is estimated to cost India in the range of thousands of crores every year. Cybercrime imposes significant as well as regressive costs on various businesses, consumers and public institutions.

The Information Technology Act 2000 and subsequent 2008 amendments make up the legal regime on Cyber Crime in India. This legal regime was framed for a digital space far less complex and threat-intense than today. The widening gap in the legal framework's design assumptions and the threat ecosystem is driven by the convergence of multiple new technological trends, each of which presents a distinct cybersecurity challenge that current frameworks do not adequately address. A serious and growing governance deficit in cybersecurity could pose major threats to India's national security, economic development and citizen welfare.

This study examines this governance deficit systematically analysing the principal emerging cybersecurity trends confronting India, assessing the legal framework's response to each, drawing comparative lessons from international experience, and advancing evidence-based recommendations for reform. The analysis is based on the view of effective cyber security governance not merely as a technical problem but fundamentally as a legal, institutional and policy problem whose solution requires a comprehensive change of law on the same scale as the problem.

II. THE EVOLVING CYBER THREAT LANDSCAPE IN INDIA

A. From Opportunistic to Strategic Threats

In past decade, cyber threat landscape of India has undergone a fundamental change. A decade ago, Indian organisations faced three significant cyber threats. To begin with, website defacement attacks, largely carried out by low-skill ideologically motivated actors. Furthermore, opportunistic malware distribution attacks, primarily targeting consumers and small businesses. And lastly, basic phishing attacks exploiting the Indian internet user base's naivety. The disruptions caused by these threats were manageable through an uncomplicated legal and institutional structure, and there were little consequences beyond the organisation directly affected.

Day by day, India faces a much more deadly threat environment. Ransomware gangs are steadily ramping up attacks against Indian organisations and establishments. These are not rogue hackers acting alone. Rather, they are well-organised groups putting together attacks like never before. The Indian government has stated that Chinese and Pakistani hacker groups

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

VOLUME 6 AND ISSUE 8 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

continue to target it. These hackers are said to be top-notch in their game and have been targeting our defense systems for a long time. India's software supply chains and the digital ecosystem as a whole are evidently vulnerable to sophisticated exploitation. Attacks involving trusted software update mechanisms to compromise thousands of downstream victims through a single point of compromise are termed supply chain attacks.

The magnitude of recorded cyber incidents reflects the scale of the problem. CERT-In put on record more than 1.3 million incidents in 2022, which is a staggering rise from around 53,000 incidents in 2017. Reserve Bank of India has recorded consistently large increases in financial sector cyber fraud as digital payment fraud alone imposes direct costs of several thousand crores each year on Indian consumers and financial institutions. Various large-scale ransomware assaults have hampered vital public services; most notably, the attack on AIIMS Delhi in November 2022 disabled the hospital's digital systems for about three weeks, affecting the data of 3-4 crore patients between 2000 and 2022.

B. Ransomware: The Most Immediate Enterprise Threat

Ransomware is the most damaging cyber threat, in terms of both impact and costs, to Indian businesses, public institutions, and critical infrastructure operators. India has gradually progressed from relatively unsophisticated commodity ransomware affecting personal computers to a stage where cybercriminals conduct sophisticated, focused operations targeting big businesses with the aim of causing maximum damage and collecting maximum ransom. This is known as "big-game hunting" in cybersecurity parlance.

The November 2022 attack on AIIMS Delhi is the most serious ransomware incident recorded in India's cyber history. Indian intelligence suggests a China-linked threat actor is blamed for the cyber attack on the All India Institute of Medical Sciences (AIIMS). The attack resulted in disruption of hospital activities for three weeks, reverting to manual operation, and compromising sensitive records.

The attack stood as a clear statement of the danger of ransomware attacks on health infrastructure. It delayed treatments, blocked diagnostics, and scrambled patient records at a major tertiary care facility serving hundreds of thousands of patients annually.

Assault on AIIMS was not isolated. The April 2022 attack on Oil India Limited asked for ransom of about $7.5 million. In May 2022, SpiceJet operations disruption and flight tracking were made impossible. The state government systems of many states have been hacked, disrupting public services and exposing citizen data. Although the banking and financial sphere has better cyber security practices than others, it too witness significant incidents of ransomware with cooperative banks and smaller financial institutions most affected.

India's legal response to ransomware falls short in a number of crucial respects. The formal legal basis for prosecuting ransomware perpetrators is provided by sections 66 and 43 of the IT Act, 2000, which criminalise hacking and provide for civil liability, respectively. Criminal prosecutions are virtually impossible in the vast majority of instances because it is extremely difficult to pin down the identity of a particular perpetrator operating through anonymized infrastructure across multiple foreign jurisdictions. India's regulatory framework is ill equipped to deal with the ransom payment issue. The legality of paying a ransom to foreign criminals, the sanctions compliance issues and the reporting obligations when ransom payments are made are not clear. This leaves organizations in a situation of maximum operational pressure and maximum legal ambiguity.

C. State-Sponsored Cyber Threats

The most strategically significant and legally complicated aspect of India's cyber security challenge is that which is sponsored by the state. China and Pakistan, state-sponsored threat

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

VOLUME 6 AND ISSUE 8 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

actors, are engaged in increasingly persistent and sophisticated cyber operations against India. Such threat actors use resources and technical sophistication that exceed those of criminal groups. India's defence research, nuclear and space establishments, government networks, and critical infrastructure systems have been the targets of these malicious cyber operations.

The RedEcho threat actor is publicly assigned Chinese state sponsorship by cybersecurity firm Recorded Future in February 2021. It attempted extensive intrusions in the power sector of India after the Galwan Valley border clash in 2020. There are network intrusions in Hindustan Power's NTPC Vindhyachal plant and regional load despatch centres. As reported by Recorded Future, the active campaigns conducted by the threat actor known as RedEcho involved the covert pre-positioning of malware on Indian power grid networks. The most hotly contested question in contemporary international cybersecurity law is whether these pre-positioning operations amount to violations of international law as uses of force, or violations of sovereignty under the UN Charter.

One of the biggest gaps in India's cyber security governance is the legal regime to respond to state-sponsored cyber operations. The IT Act 2000 does not deal with state-sponsored cyber operations. The stipulations in Section 66F regarding cyber terrorism that demand an intent to "strike terror" are ill-suited to state-sponsored strategic objectives. India's current framework lacks or inadequately defines clear legal authorities for conduct of active cyber defence operations in foreign territory, standards for attribution and options for diplomatic and legal accountability.

D. Artificial Intelligence and Cybersecurity: The Dual-Use Challenge

Artificial intelligence is changing the cybersecurity landscape in all aspects from generating new threats to strengthening defence and raising new regulatory issues. AI technology is aiding in qualitative improvements to offensive capabilities relevant to India. Phishing powered by AI which uses large language models to generate highly personalised, contextually accurate messages in several Indian languages such as Hindi, Telugu, Tamil and Bengali will significantly boost the effectiveness of social engineering against users who could be snowed under with carefully crafted messages in their mother tongue. AI-powered adaptive malware that modifies its behaviour to easily evade signature-based detection presents a major challenge to widely used security tools in India.

The technology that employs AI to make fake video and audio with a high degree of accuracy has been weaponized in India in several documented cases. The capability to generate phoney CEO voices from limited data facilitates the so-called CEO fraud where fake voice recordings convince company finance officers to make dubious wire transfers. With rapid improvements in the reality of the deepfakes and the availability of easier tools for generation, this attack vector can be especially harmful.

In India, there is a significant regulatory vacuum in the legal framework for AI-enabled cyber attacks. There are no provisions in the IT Act for AI-enabled attacks, AI-generated disinformation, and security requirements of AI systems for critical applications. Whether deepfake fraud falls within the ambit of identity theft under Section 66C, which penalises dishonest use of another person's electronic identification, is a question of construction not yet systematically addressed by Indian courts.

E. Internet of Things: The "Insecure by Design" Problem

India's thriving IoT ecosystem – from the smart city infrastructure in over 100 Smart Cities Mission cities to industrial control systems, connected healthcare devices, agricultural monitoring systems, and hundreds of millions of consumer devices – is among the biggest and most under-addressed cybersecurity threat. Majority of IoT devices are designed for minimum security: with default or hardcoded passwords, firmware that

cannot be patched remotely, little encryption and no security monitoring. Security features add to the cost. Yet consumers in electronics markets have shown that buyers are not that will to pay for them.

The emergence of botnet or 'zombie' armies of compromised Indian IoT devices is a serious problem with domestic and international ramifications.

In 2016, the Mirai botnet showed how many IoT devices using default credentials could be recruited to create huge DDoS attack infrastructure. The new IoT botnets exploited the same or similar vulnerabilities with increasing sophistication and recruited Indian devices to attack global targets.

The legal framework of India for IoT security is fragmented. IS 17897:202 IoT security standard of Bureau of Indian Standards will provide useful technical guidance but is not mandatory. In principle, the general computer security provisions of the IT Act would apply to IoT, but it does not mention any device-specific security requirements. The consequence of this is that despite facing systemic IoT security risks, Indian consumers and businesses do not benefit from the existence of mandatory minimum standards that could create market incentives for manufacturers to improve product security..

F. Cloud Computing, 5G, and Emerging Threats

The data security landscape is changing as the Indian Government and private corporations move data to the cloud at an alarming rate. Cloud misconfiguration constitutes the most common and harmful cloud security threat. As the report explains, a cloud misconfiguration refers to exposure of cloud storage and databases with incorrect security settings. It has been implicated in several major data breaches of late, wherein hackers accessed sensitive personal and financial information of millions of users in India. India lacks mandatory cloud security standards and configuration auditing requirements. This means the vulnerability remains substantially unaddressed.

Following spectrum auctions in July 2022 and gradual rollout by major operators, India's 5g deployment brings new cyber security challenges. The broad-spectrum 5g architecture of softwarised design introduces new cyber technology challenges. The effective exclusion of Chinese equipment vendors Huawei and ZTE from India's 5G networks effected via informal government guidance rather than the transparent, rule-based regulation reflects legitimate security concerns but lacks the formal legal framework akin to the UK's Telecommunications (Security) Act 2021 that would ensure consistent, transparent, and judicially reviewable implementation.

III. INDIA'S CYBERSECURITY LEGAL FRAMEWORK: A CRITICAL ASSESSMENT

A. The Information Technology Act 2000: Strengths and Limitations

In India, the principal law for cybersecurity and cybercrime is the Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008. The key cybersecurity provisions in the Act include Section 43, which imposes civil liability for wrongful computer access and data theft; Section 66, which makes dishonest or fraudulent computer access a criminal offence; Sections 66A to 66F, which deal with specific cybercrimes like identity theft and cyber terrorism; Section 70, which allows for the designation of protected systems; and Section 70A, which establishes CERT-In as the national agency for cybersecurity.

Although these provisions of law provide a good framework, they are structurally inadequate to deal with the emerging threats. The definitional structure of the Act, which was drafted over two decades back in 2000, does not contain anything specific about IoT devices, industrial control systems, AI systems, cloud infrastructure of things, etc. The absence of definitions creates an ambiguity of interpretation about whether and how the key provisions of the Act deal with IoT devices and other technologies. The provisions around criminal offence indicates the threat environment of their time. For example, we

made laws against hacking and data theft but did not create laws against ransomware, deepfakes, cyber fraud using AI, and attacks on supply chain. Many provisions' penalties will not deter sophisticated international criminal organisations or large corporations with inadequate security practices.

There are issues related to the effectiveness of the enforcement of the Act. Even though India has provisions for criminal offence against cybercrime there has only been an insignificant success rate in prosecution of cybercrime. This is attributed to inadequate forensic capacity in majority of state police forces; lack of adequate specialised expertise to prosecute these cases; and almost no possibility of prosecuting perpetrators in foreign jurisdictions through existing mutual legal assistance mechanism. The gap between the law and the real situation creates a gap between the law and real situation.

B. The Digital Personal Data Protection Act 2023

The Digital Personal Data Protection Act 2023 is the most important recent legislation in India in the field of cybersecurity, which establishes a legal framework for personal data protection with important cybersecurity consequences. According to Section 8(5), data fiduciaries must take reasonable security safeguards to prevent breaches of personal data. This is a broad security obligation which applies all data fiduciaries regardless of sector or size. The provisions of the Act requiring a breach notification to the Data Protection Board and the affected data principals in the event of a personal data breaches represent a significant enhancement of India's data security incident management framework.

Though, the Act suffers from important limitations as a cybersecurity instrument. The high-level security obligations do not specify the technical standards that constitute what is meant by "reasonableness" in different contexts, leaving regulated entities uncertain about what is expected of them, limiting the basis on which enforcement could happen. At the time of this writing, the implementing rules that set out the precise timing, content and procedures for breach notifications had not been finalised. The maximum penalty of INR250 crore is substantial as per Indian laws but is very small as compared to the GDPR which provides for a maximum penalty of EUR20 million or 4% of global annual turnover. Such a penalty might not be a disincentive for big global players. The DPDP Act is primarily concerned with regulation of data not cybersecurity. There is no provision for security of critical infrastructure and IoT security standards or the government investigation and response powers that comprehensive cybersecurity governance requires.

C. CERT-In Directions 2022 and Institutional Architecture

Regulatory development requires a cybersecurity incident report. The CERT-In Directions of April 2022 represent the most significant recent regulatory development in India's cybersecurity framework. They make mandatory the reporting of no less than 20 categories of cybersecurity incidents, no later than six hours of detection. ICT system logs must also be retained for 180 days. ICT system clocks must be maintained accurately, synchronised with the NTP server of the National Informatics Centre or National Physical Laboratory. Further, virtual private network providers must maintain subscriber and customer records.

The Directions are a substantial step towards comprehensive regulation. Yet they have been criticised on several grounds. The six-hour reporting window has been widely criticized as operationally unrealistic in the wake of complex incidents where even basic incident characterisation may not be achievable within that time frame. This requirement is more compressed than that of the EU NIS2 Directive (24 hours), CIRCIA (72 hours) or Singapore (two hours, critical infrastructure only). VPN logging rules that require VPN providers to keep extensive subscriber records are resulting in the withdrawal of Indian server infrastructure by various leading VPN providers rather than

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

compliance, which may compromise the security of Indian users who rely on VPNs to keep their privacy safe.

India has an institutional arrangement for cybersecurity which shares out responsibilities among CERT-In under MeitY, NCIIPC under the National Technical Research Organisation, the National Cyber Security Coordinator housed in the National Security Council Secretariat, sectoral regulators, etc. But this arrangement suffers from poor coordination, ambiguity of jurisdictions, and no unified incident command structure for major cross-sector incidents. The insufficient coordination among investigation agencies, IT ministries, and telecom regulators causes a reduction in India's cybersecurity response speed and coherence.

IV. COMPARATIVE ANALYSIS: INTERNATIONAL CYBERSECURITY FRAMEWORKS

A. The European Union: A Comprehensive Mandatory Framework

The European Union's Cybersecurity Regulatory Framework which is based on the NIS2 Directive (Directive (EU) 2022/2555) and the EU Cybersecurity Act (Regulation (EU) 2019/881) is the most comprehensive mandatory cybersecurity regulatory framework of any jurisdiction in the world. The NIS2 Directive requires essential and important entities across a range of sectors to take risk management measures covering specific security areas, which include incident handling, supply chain security, access control, encryption; reporting of material incidents to their national authority within 24 hours upon detection; and the possession of business continuity plans for cyber incidents. The enforcement regime of the Directive obliges member states to ensure that relevant authorities are in place that can impose administrative fines of up to €10 million of 2% of global annual turnover for essential entities. It creates a material financial incentive to comply with cybersecurity provisions.

The EU Cybersecurity Act established a cybersecurity certification framework for ICT products, services, and processes where achieving standardised assurance levels demonstrates compliance with defined security requirements. The Cyber Resilience Act, which is advancing through the EU legislative process, would make it mandatory for manufacturers of connected devices to follow security requirements. For example, manufacturers will have to develop and release updates to ensure a device is secure by design throughout the supported lifetime of the device. Thus, these instruments create a more comprehensive regulatory architecture that addresses both organisational security practices and product security, unlike what India has so far.

B. The United States: Sector-Specific Standards and Voluntary Frameworks

The approach that the United States takes when it comes to governance of cybersecurity consists of a mix between mandated standards that deal with specific sectors like the NERC CIP standards for electricity, HIPAA Security Rule for the health sector, and PCI-DSS for payment cards. Another aspect of this same framework is the NIST Cybersecurity Framework which acts as a cross-sector reference, this framework is quite voluntary though. And recently, there are increasing mandated requirements that are taking shape through legislation that is being passed. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) 2022 established mandatory 72-hour incident reporting requirements for critical infrastructure operators, the first comprehensive cross-sector mandatory reporting framework, while the IoT Cybersecurity Improvement Act 2020 created minimum security requirements for IoT devices used by federal agencies.

The major strength of the approach of USA is its developed public-private partnership infrastructure, including Information Sharing and Analysis Centres for every critical sector, the Joint Cyber Defense Collaborative, and the engagement programmes of CISA that creates effective mechanisms for sharing intelligence about threats between government and private

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

VOLUME 6 AND ISSUE 8 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

sector operators. A significant setback of the global architecture is the fragmentation which persists across various agencies and frameworks specific to each sector. A seamless unified architecture would have ensured greater cross-sector coordination during major incidents.

C. Singapore: The Most Relevant Asian Model

The Cybersecurity Act 2018, which was implemented by the Cyber Security Agency, establishes Singapore's cybersecurity governance framework. Singapore's approach is arguably the most directly relevant international model for India, as it has the comprehensive legislation, strong institutional capacity, and effective public-private partnership to be found within a legal tradition and developmental context that is arguably the most comparable to India's.

The Cybersecurity Act creates a framework for: the designation and protection of Critical Information Infrastructure in eleven critical sectors; a licensing framework for cybersecurity service providers; wide investigative and enforcement powers for the Commissioner of Cybersecurity; a two hour incident reporting requirement on CII owners; compulsory cybersecurity exercises; and provisions for international cooperation. The layered legislative architecture that combines CII protection and the regulation of service providers along with investigative powers of government in one statute will provide coherence and comprehensiveness that is lacking in India's fragmented multi-statute framework.

The Singapore CII protection scheme which imposes on designated CII owners the duty to comply with codes of practice specifying detailed technical security requirements, conduct risk assessments and audits on a regular basis, and maintain business continuity plans provides a model for the sectoral-specific mandatory security standards that India's reform agenda should prioritise. With the systematic development of talent, government scholarships for cybersecurity study, and industry certification frameworks, Singapore's investment in cybersecurity workforce development is similarly a way to address India's severe cybersecurity skills shortage.

V. CRITICAL EVALUATION AND REFORM RECOMMENDATIONS

A. The Cybersecurity Governance Deficit: A Structural Assessment

As India's cyber threat landscape transforms, the study of the law reveals a cybersecurity governance deficit of serious and growing proportions. Indeed, there are four main types of deficits.

The dimension of legislative obsolescence concerns the IT Act 2000's fundamental inadequacy for contemporary threats – its definitional framework predates IoT, AI, cloud and sophisticated ransomware; its offence provisions do not specifically cover the most consequential contemporary threat categories; and its enforcement mechanisms are inadequate for the cross-border, technically complex character of modern cybercrime. A piecemeal modification cannot take care of these systemic shortcomings. It is needed a comprehensive legislative overhaul through a dedicated National Cyber Security Act.

The institutional fragmentation dimension refers to a situation where multiple agencies are assigned cybersecurity responsibilities, but there is no effective coordination, clear jurisdictional delineations, or unified incident command structures. This fragmentation makes responses ineffective at a time when coherence matters most during big multi-sector incidents with cascading impacts across interlinked digital infrastructure.

The absence of or inadequacy of regulatory frameworks for emerging technology categories IoT security, AI system security, 5G supply chain security, and cryptocurrency cybersecurity is the subject matter of the regulatory gap dimension of this paper each of which creates significant and documented vulnerabilities but to which the

legal framework in India does less than sufficient response.

The dimension of enforcement gap relates to the persistence and magnitude of the gap between the formal cybercrime legal framework in India and its effective enforcement in practice, as evidenced by extremely low prosecution rates, which do not create any deterrence impact on sophisticated cybercriminals.

B. Principal Reform Recommendations

Based on analytical findings and comparative lessons, the article makes the following key reform recommendations.

India must quickly adopt a National Cybersecurity Act that streamlines and updates India's Cybersecurity laws. The Act must create a clear definitional framework which encompasses contemporary computing and other technologies; mandatory security requirements for critical information infrastructure operators; a licensing framework for cybersecurity service providers; updated criminal offence provisions that expressly address ransomware, deepfakes, AI-enabled fraud and state-sponsored cyber-attacks; wide-ranging government investigation and enforcement powers; and clear public-private partnership mechanisms. 2018 Cybersecurity Act of Singapore provides the most relevant legislative model.

Furthermore, India should establish obligatory security standards tailored to each designated critical information infrastructure sector, which consist of power, banking, telecom, health care, transport, government. The standards should be technically specific, updated regularly through a defined review process, and subjected to mandatory compliance verification through periodic audits. The most relevant comparative models come from the EU's NIS2 Directive's sector-specific approach and from Singapore's codes of practice.

Third, India must create a National IoT Security Framework which will lay down mandatory minimum security requirements for any IoT device that is sold or deployed in India, starting with devices in critical infrastructure and smart city applications, and gradually extending to consumer devices. All default passwords that can be applied universally should be made illegal. Further, there should be mandatory provisions for the security updates. Moreover, the minimum period of support should also be disclosed. Moreover, there must be registration of all imported items under a national IoT security registry.

India must create a National Cyber Security Agency to include functions of CERT-In and NCIIPC. The fourth step in government's cyber security framework must create such an institution with clear statute, adequate resourcing and accountability. India's nodal agency for civil and critical info structure cyber security for unified agency. It should coordinate through coordinating mechanisms and law through sector regulators, law enforcement agencies and intelligence forces.

India ought to amend the CERT-In Directions to supplant the six-hour single-stage reporting obligation with a tiered notification regime an initial 24-hour notification, a detailed 72-hour report and a final analysis in 30 days modelled on the EU NIS2 model. The incident response operational realities balance the legitimate needs of government to achieve timely situational awareness in which this tiered framework operates.

India needs to develop a National CyberSecurity Workforce Development Strategy that contains systemically mandatory cyber security curriculum elements in computer science programmes, Government funded cyber security scholarships, a national certification framework, Government apprenticeship programmes, etc. A shortage of several hundred thousand cyber security professionals restricts the effectiveness of regulatory frameworks and organisational security practices.

India needs to make a framework on 5G supply chain security Seventh characterized by transparency, rules, criteria and processes for

assessing security risks related to network equipment and software from different vendors, provides legal certainty for network operators and a principled basis for vendor risk assessments that can withstand judicial scrutiny.

VI. CONCLUSION

India's Cybersecurity Governance Development Is At A Critical Juncture. India is experiencing an extraordinary level of digitalization. This has created transformative economic and social opportunities. At the same time, it has placed the country at serious cyberspace vulnerabilities that the legal, regulatory and institutional mechanisms are inadequate to meet.

Implementation of 5G technology, increasing usage of Artificial Intelligence, successful Remote Desktop Protocol attacks and other ongoing trends will shape the future threat landscape so let's analyze it.

The Indian statutory system based on a 25-year old more or les statute aimed at a different kind of threat cannot work in this environment through simple amendments. The challenge of cyber insecurity arises from the intersection of three forces: technology, business and governance. What is needed is comprehensive legislative reform: a National Cybersecurity Act to deliver a coherent, comprehensive, and technically up-to-date legal framework; mandatory regulatory standards for critical infrastructure at the sector level with standards aligned to the threat sophistication levels faced by that sector; sectorally-aligned regulatory frameworks for emerging technologies with security obligations created where none exists presently; and institutional reshaping which delivers the coordination, capacity and accountability which effective cybersecurity governance requires.

The European Union, the United States and Singapore present comparative experience each having invested systematically in developing exhaustive cybersecurity governance framework. Effective cybersecurity governance is possible with sufficient political will and sustained investment. India's technical skills, institutional foundations, and policy recognition of cybersecurity's importance can help create expert governance in the area. Conveying this recognition into legislative action and institutional investment commensurate with the scale of India's cybersecurity challenge and the scale of the economic and security consequences of failing to meet it is the challenge.

REFERENCES

Abbott, F.M. (2005) The WTO Medicines Decision. American Journal of International Law, 99(2), pp. 317–358.

Borghard, E.D. and Lonergan, S.W. (2017) The Logic of Coercion in Cyberspace. Security Studies, 26(3), pp. 452–481.

CERT-In (2022) Directions Under Sub-Section (6) of Section 70B of the Information Technology Act 2000. New Delhi: Ministry of Electronics and Information Technology.

CERT-In (2023) Annual Report 2022-23. New Delhi: Indian Computer Emergency Response Team.

Chesney, R. (2018) Cybersecurity Law, Policy and Institutions. Austin: University of Texas School of Law.

Christou, G. (2016) Cybersecurity in the European Union. Basingstoke: Palgrave Macmillan.

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (2022) Pub. L. No. 117-103.

Cybersecurity Act 2018 (Act No. 9 of 2018). Singapore.

Data Security Council of India (2022) India Cyber Threat Report 2022. New Delhi: DSCI.

Deibert, R. (2020) Reset: Reclaiming the Internet for Civil Society. Toronto: Anansi.

Digital Personal Data Protection Act 2023 (Act No. 22 of 2023). India.

Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity (NIS2 Directive) [2022] OJ L333/80.

Duggal, P. (2014) Textbook on Cyber Law. New Delhi: Universal Law Publishing.

European Commission (2022) Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act). COM(2022) 454 final.

Healey, J. (ed.) (2013) A Fierce Domain: Conflict in Cyberspace 1986-2012. Washington, DC: Atlantic Council.

Information Technology Act 2000 (Act No. 21 of 2000), as amended 2008. India.

Institute for Security and Technology (2021) Ransomware Task Force: Stopping Ransomware. Washington, DC: IST.

International Telecommunication Union (2021) Global Cybersecurity Index 2020. Geneva: ITU.

Klimburg, A. (2017) The Darkening Web: The War for Cyberspace. New York: Penguin.

Maschmeyer, L., Deibert, R. and Lindsay, J.R. (2021) A Tale of Two Cybers. Journal of Information Technology and Politics, 18(1), pp. 1–15.

Ministry of Electronics and Information Technology (2013) National Cyber Security Policy 2013. New Delhi: Government of India.

Mueller, M. (2010) Networks and States: The Global Politics of Internet Governance. Cambridge, MA: MIT Press.

NASSCOM and DSCI (2022) India Cyber Threat Report 2022. New Delhi: DSCI.

Nappinai, N.S. (2011) Cyber Crime Law in India. New Delhi: Universal Law Publishing.

National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Gaithersburg, MD: NIST.

NCIIPC (2021) Guidelines for Protection of Critical Information Infrastructure. New Delhi: NCIIPC.

Recorded Future (2021) China-Linked Group RedEcho Targets the Indian Power Sector. Somerville, MA: Recorded Future.

Regulation (EU) 2019/881 on ENISA and on ICT Cybersecurity Certification (EU Cybersecurity Act) [2019] OJ L151/15.

Reserve Bank of India (2016) Cyber Security Framework in Banks. RBI/2015-16/418. Mumbai: RBI.

Rid, T. (2013) Cyber War Will Not Take Place. London: Hurst Publishers.

Schmitt, M.N. (ed.) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.

Singer, P.W. and Friedman, A. (2014) Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press.

Telecommunications (Security) Act 2021 (c. 31). United Kingdom.

UN Group of Governmental Experts (2015) Report A/70/174. New York: United Nations.

Zetter, K. (2014) Countdown to Zero Day. New York: Crown Publishers.

INSTITUTE OF LEGAL EDUCATION

(Managed by L TO J LAW ASSOCIATES)

NO. 08, ARUL NAGAR, SEERA THOPPU,
MARUDHAANDA KURICHI, SRIRANGAM - 620102,
TAMILNADU, INDIA.

ISSN 2583-2344