Akshara Gupta, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

India's National Cybersecurity Strategy (2020 Draft): Gaps Between Policy and Law

Akshara Gupta
Institutional Affiliation: School Of Law, Galgotias University

Abstract- The frequency, sophistication, and intensity of cyber-attacks have compelled strong national cybersecurity efforts worldwide. India being among the largest digital economies is confronting special cybersecurity challenges in terms of cybercrime, data breaches, vulnerabilities in infrastructure as well as issues regarding digital sovereignty. The Ministry of Electronics and Information Technology (MeitY), anticipating this challenge and responding to it, formulated the National Cybersecurity Strategy (NCS) in 2020. Though the draft gives an overarching vision including secure cyberspace, data privacy as well as institutional coordination, it shows gaps galore when tested against current legal norms and principles. This paper critically examines the 2020 draft National Cybersecurity Strategy (NCS) by contrasting its goals with India's existing legislative and regulatory framework, including the Information Technology Act 2000, the Personal Data Protection Act (DPDP), 2023, and industry-specific policies. The research reveals major policy-law disconnects including a lack of legally enforceable commitments, institutionally fragmented accountability, inadequate cyber deterrent provisions, and insufficient transparency regarding surveillance and privacy protections. Additionally, the draft strategy is lacking in specific timeframes, implementation mechanisms, and convergence with international norms and conventions on cybersecurity. Through doctrinal legal assessment and policy examination, the paper analyzes how gaps might jeopardize India's cybersecurity posture and international digital credibility. The study culminates with policy proposals for legal reform, inter-agency coordination structures, and institutionalizing cybersecurity audits to implement the strategy efficaciously. Closing the gap between policy aspiration and enforceable law is necessary to maintain India's cyberspace resilient, secure, and rights-respecting amidst rising digital threats.

Keywords - Key Words: Cybersecurity, National Cybersecurity Strategy, India, Cyber Law, IT Act 2000, Data Protection, Policy-Legal Gap, Digital Sovereignty, meitY, Cybercrime

I. INTRODUCTION

The rapid digitization of India's economy and governance systems has elevated cybersecurity to a matter of national concern. With over 800 million internet users and expanding reliance on digital infrastructure, India is increasingly vulnerable to a spectrum of cyber threats ranging from financial fraud, critical infrastructure attacks, and digital espionage to cyberterrorism. In light of these escalating risks, the Indian government released the National Cybersecurity Strategy (NCS) draft in 2020, aimed at consolidating the country's fragmented cybersecurity landscape into a unified, future-ready framework.

While the strategy aspires to secure the digital ecosystem, enhance cyber awareness, and promote indigenous cybersecurity capabilities, it falls short in providing a robust legal backing to these objectives. Scholars have widely acknowledged that the legislative foundation of India's cybersecurity framework, principally the Information Technology Act, 2000—is outdated and ill-equipped to address contemporary cyber threats . In addition, India lacks a comprehensive data protection regime despite the recent enactment of the DPDP Act, 2023, leaving a regulatory vacuum concerning privacy, consent, and data governance .

The Indian cybersecurity legal ecosystem has been described as a patchwork of sectoral regulations and ad hoc guidelines that suffer from jurisdictional ambiguity, insufficient enforcement powers, and inconsistent implementation . Furthermore, the strategy does not provide for clear timelines, statutory mandates, or enforcement agencies, resulting in a policy that is aspirational but unenforceable. Comparative research highlights how technologically advanced nations have bridged similar policy-legal gaps through strong legislative mandates, national standards, and multi-stakeholder governance models . India's NCS 2020 draft also lacks provisions for global cooperation, despite the increasingly transnational nature of cybercrime . This has prompted concerns regarding India's readiness to align with global norms and engage in cross-border cybersecurity diplomacy.

Moreover, scholars argue that India's cybersecurity posture remains reactive, primarily responding to high-profile breaches rather than proactively institutionalizing resilience frameworks . India must transition from policy narratives to legally enforceable instruments that clearly delineate institutional responsibilities, rights protections, and accountability mechanisms .

This paper critically examines these issues by analysing the key provisions of the NCS 2020 draft and comparing them with India's prevailing cyber laws and institutional capacity. It identifies specific legal gaps, evaluates the implications of an unenforceable strategy, and offers practical reforms to bridge the gap between policy ambition and legal enforcement.

II. UNDERSTANDING THE NATIONAL CYBERSECURITY STRATEGY 2020

India's National Cybersecurity Strategy (NCS) 2020 draft, formulated by the National Security Council Secretariat (NSCS), represents a landmark effort to develop a comprehensive and coordinated approach to address the country's rapidly evolving cyber threats. Recognizing the strategic significance of cyberspace in India's economic and national security architecture, the draft proposes a forward-looking policy framework structured around three key pillars: Secure, Strengthen, and Synergize.

Under the "Secure" pillar, the strategy emphasizes the protection of critical information infrastructure (CII), government digital systems, and national data assets. It proposes enhanced threat intelligence capabilities, periodic audits, and sector-specific cybersecurity standards.

The "Strengthen" component focuses on building indigenous cybersecurity capabilities through investments in R&D, workforce development, and public-private collaboration. Finally, the "Synergize" pillar underscores the need for institutional coordination, capacity building among law enforcement agencies, and international cooperation.

Despite its well-structured layout and strategic clarity, scholars argue that the NCS 2020 falls short in several key areas.The strategy for being policy-heavy but legally weak, noting that it lacks statutory backing or a clear mandate for enforcement . Similarly, the document remains non-binding, and is yet to be notified or formally adopted as government policy, raising serious questions about its operational feasibility .

The NCS 2020 also fails to address jurisdictional overlaps and institutional fragmentation. India's cybersecurity regime suffers from a lack of centralized authority and poor coordination among agencies such as CERT-In, NCIIPC, and MeitY . While the strategy mentions coordination, it does not specify how such integration will be implemented legally or structurally.

A key limitation lies in the absence of enforceable obligations. India's current legal foundation—mainly the Information Technology Act, 2000—does not provide the legislative support needed to implement the strategy's ambitious goals. Without amendments to existing laws or the introduction of a dedicated cybersecurity statute, the strategy's impact will remain aspirational .

From a comparative lens, India lags behind countries like the U.S. and EU, where cybersecurity strategies

are embedded within enforceable legal frameworks. The most effective national strategies involve legislative integration, agency accountability, and regular compliance mechanisms. Reinforce this view, suggesting that legal enforceability is the missing link in many developing countries' cyber strategies, including India .

Moreover, India's strategy appears inward-looking and insufficiently global in scope. In an era of cross-border cyber threats, national strategies must incorporate robust frameworks for international cooperation and cyber diplomacy, which the NCS 2020 only briefly mentions .

The absence of synergy between cybersecurity and data protection is another concern. India's data protection regime remains incomplete, and without legal integration between data governance and cybersecurity, policy coherence cannot be achieved. The strategy must go beyond threat mitigation and embed resilience into the digital public infrastructure itself.

The NCS 2020 is a critical milestone in India's cyber policy journey, its current form remains largely declarative. The lack of legal enforceability, institutional clarity, and global alignment highlights the urgent need for reforms that transform policy vision into actionable law.

III. LEGAL AND INSTITUTIONAL LANDSCAPE OF CYBERSECURITY IN INDIA

India's legal and institutional framework for cybersecurity is rooted in a reactive and fragmented model, primarily shaped by the Information Technology Act, 2000 (IT Act) and administered through a web of agencies with overlapping mandates. While this framework has evolved over the years to incorporate certain cybercrime and data protection provisions, it remains ill-equipped to support the broad objectives of the National Cybersecurity Strategy (2020 draft).

The IT Act, 2000 remains the principal legislation governing cyber activities in India. It provides a legal framework for electronic commerce, cybercrime, and digital signatures. However, the Act was never envisioned as a comprehensive cybersecurity law. It lacks robust provisions on critical infrastructure protection, cyber deterrence, and mandatory security compliance for private and public sector entities. While Sections 66 to 74 address cyber offences, these are largely criminal in nature and do not set standards for cyber risk mitigation, audit, or incident response .

Tthe Act's piecemeal amendments over time have not kept pace with the complexities of contemporary cyber threats such as ransomware, state-sponsored attacks, and AI-driven intrusions . The absence of targeted provisions for cybersecurity governance and inter-agency coordination is a glaring gap that undermines the effectiveness of the IT Act as a cybersecurity instrument.

In the absence of a unified cybersecurity law, India has relied on sectoral regulations to manage cybersecurity. Regulatory authorities such as the Reserve Bank of India (RBI), Telecom Regulatory Authority of India (TRAI), and Insurance Regulatory and Development Authority of India (IRDAI) have issued guidelines to govern cyber practices within their respective domains. However, these operate in silos and often lack enforceability or harmonization. This fragmented approach has led to regulatory overlaps and confusion, especially in the wake of major cyber incidents that require cross-sector coordination. The absence of a lead cybersecurity agency capable of issuing binding norms across sectors severely weakens India's cyber-resilience .

India's cybersecurity responsibilities are distributed among various institutions. The Ministry of Electronics and Information Technology (MeitY) oversees policy, while CERT-In (Indian Computer Emergency Response Team) is the national nodal agency for cyber incident response. NCIIPC (National Critical Information Infrastructure Protection Centre), under the National Technical Research Organisation (NTRO), is tasked with protecting critical infrastructure.

However, this model as administratively fragmented and lacking in centralized oversight. The roles and responsibilities of these institutions often overlap, leading to conflicts of jurisdiction and delayed responses during cyber emergencies .

Similarly, the absence of a statutory body dedicated exclusively to cybersecurity, arguing that India's institutional framework lacks the scale, autonomy, and authority to handle large-scale cyber threats . This has often resulted in ad hoc and event-driven policy responses, rather than sustained strategic execution.

A major institutional and legal shortcoming in India's cybersecurity architecture is its weak integration with data protection mechanisms. While the Digital Personal Data Protection Act, 2023 (DPDP) now provides a framework for personal data regulation, it is yet to be fully operationalized. India's failure to synchronize cybersecurity and data protection laws leaves significant gaps in securing citizens' rights and trust in digital infrastructure .

A robust cybersecurity regime must include cross-linkages with privacy, surveillance, and civil liberties to be effective in the long run. However, such linkages are either absent or ambiguously defined within current Indian laws .

Global practices further highlight the inadequacies of India's current framework. Countries with successful cybersecurity strategies—such as the U.S. and Germany—have codified national cybersecurity laws and clear institutional hierarchies . Even countries Pakistan has moved toward centralizing cybersecurity governance under formal legal mandates, underscoring India's relative inertia in legal reform .

Moreover, that India's fragmented domestic architecture also hampers its ability to participate in global cybersecurity cooperation, since no single agency has the authority or mandate to represent the country in transnational forums effectively .

India's cybersecurity legal and institutional landscape is characterized by regulatory fragmentation, outdated legislation, and weak institutional synergy. While individual agencies perform specific roles, the lack of a unified, enforceable, and forward-looking legal framework hampers India's capacity to respond to sophisticated and evolving cyber threats. Bridging this gap requires not just strategic vision but structural reforms, legal integration, and institutional consolidation, without which the National Cybersecurity Strategy will remain a non-operational policy artefact.

Gap Analysis – Policy Vs. Law

The National Cybersecurity Strategy (NCS) 2020 draft outlines an ambitious vision for safeguarding India's digital infrastructure and promoting cyber resilience. However, a detailed analysis reveals significant gaps between the strategic policy framework and the existing legal architecture, which severely limit the operationalization of the strategy. These gaps are visible in four critical areas: the absence of enforceable mandates, lack of legislative support, jurisdictional overlaps, and inadequate integration with international cooperation frameworks.

The NCS 2020 proposes a multi-layered approach to cybersecurity, emphasizing threat mitigation, capacity building, critical infrastructure protection, and public-private partnerships. However, the strategy is not binding, nor does it impose any legal duties on stakeholders. It is a policy document lacking statutory force, meaning that compliance by various entities, public or private, is not legally required .

India's cybersecurity strategy is based on administrative directives and sectoral guidelines, not codified law . Without a legal mandate, there is no mechanism to ensure that organizations adhere to the standards and practices envisioned in the strategy. This results in a weak compliance culture, especially among private sector actors handling sensitive data and infrastructure.

The second major gap lies in the disjointed relationship between policy objectives and India's legislative framework, particularly the Information

Technology Act, 2000. The IT Act was drafted at a time when cybersecurity threats were rudimentary and primarily financial in nature. Its provisions fail to address modern threats like cyber warfare, AI-driven attacks, or large-scale ransomware incidents

Furthermore, the absence of a dedicated cybersecurity law to support the NCS 2020 significantly weakens its effectiveness. Unlike global counterparts such as the EU's NIS Directive or the U.S. Cybersecurity Information Sharing Act (CISA), India's legal response remains fragmented, with no uniform security standards or breach notification laws embedded in enforceable statutes .

A major institutional gap identified by multiple scholars is the lack of clarity regarding the jurisdiction and responsibilities of various cybersecurity bodies. There is no designated apex cybersecurity agency to coordinate among different actors, leading to operational delays and inefficiencies during major cyber incidents .

The strategy does not delineate institutional roles with precision, which weakens India's ability to respond effectively to cross-border cyber threats and participate in global cyber diplomacy .

Drawing from international comparisons, suggest that effective strategies are always backed by centralized and empowered institutions . In contrast, India's institutional framework remains decentralized and bureaucratically fragmented, undermining the collaborative execution that the strategy seeks.

The NCS 2020 draft fails to adequately integrate with India's evolving data protection regime, especially with the enactment of the Digital Personal Data Protection Act, 2023. The absence of legal alignment between cybersecurity and data privacy frameworks dilutes individual rights protections and creates loopholes in both enforcement and accountability .

The strategy pays insufficient attention to constitutional safeguards, such as the right to privacy, and does not clarify limits on state surveillance or data retention. This raises concerns about the democratic legitimacy of the strategy's implementation .

Lastly, the NCS 2020 remains largely inward-looking. While it mentions the importance of international collaboration, it lacks actionable pathways or legal mechanisms for engaging with global partners.

The analysis reveals a clear and critical gap between India's strategic ambitions and its legal infrastructure. The National Cybersecurity Strategy (2020 draft), though conceptually robust, lacks legal enforceability, institutional cohesion, legislative integration, and global connectivity. These gaps threaten to render the strategy ineffective unless addressed through comprehensive legal reforms and policy restructuring. Bridging this divide is essential for translating cybersecurity policy into practical, enforceable outcomes that safeguard national interests while upholding democratic values.

IV. COMPARATIVE PERSPECTIVES: GLOBAL BEST PRACTICES

As cybersecurity becomes a global imperative, nations across the world have developed robust legal and institutional frameworks to address evolving digital threats. While India's National Cybersecurity Strategy (2020 draft) outlines key objectives, it lacks the legal and institutional maturity found in many technologically advanced jurisdictions. This chapter draws on comparative models from the United States, European Union, and Pakistan to extract best practices that India can adapt to bridge its policy-legal gap.

The United States offers a model of clear legal mandates, centralized oversight, and private sector coordination. Laws such as the Cybersecurity Information Sharing Act (CISA) and the Federal Information Security Modernization Act (FISMA) provide legal backing for threat sharing and cybersecurity audits across federal agencies.

The U.S. approach integrates cybersecurity policy with statutory obligations and emphasizes sector-specific standards issued by agencies such as the National Institute of Standards and Technology (NIST). This legal clarity enables timely responses to

cyber incidents and fosters a culture of proactive compliance . The success of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which acts as a central coordinating body, with both technical and legal authority . Unlike India, where CERT-In lacks enforcement powers, CISA plays a strategic and operational role, empowered by legislation.

The European Union (EU) provides an example of a cybersecurity strategy deeply embedded in both legislation and fundamental rights protections. The EU Network and Information Security (NIS2) Directive mandates member states to implement uniform cybersecurity standards and incident reporting protocols. What distinguishes the EU model is its synergistic relationship between cybersecurity and data protection laws, particularly the General Data Protection Regulation (GDPR) . This ensures that cybersecurity practices do not violate privacy rights, and vice versa, an area where India continues to fall short. The EU frameworks are supported by enforceable compliance obligations, independent supervisory authorities, and multi-stakeholder consultation processes. These mechanisms guarantee transparency, accountability, and cross-border cooperation, attributes largely absent from India's fragmented system .

In contrast to perceptions of weak governance, Pakistan has made notable legislative progress in recent years. The Prevention of Electronic Crimes Act (PECA), 2016, and its subsequent amendments have enabled law enforcement agencies to respond more swiftly to cybercrimes. Pakistan's move toward a centralized cybersecurity agency, with clear legislative authority and sectoral coordination, offers a useful parallel for India . While Pakistan's enforcement mechanisms face challenges, its progress toward an integrated cybersecurity law demonstrates the importance of legal centralization and executive will, both of which remain weak points in India's approach.

Drawing from these jurisdictions, a few common principles emerge that define global best practices:

- Legislative Codification: All effective models integrate cybersecurity strategy into binding law.
- Centralized Institutional Leadership: The presence of a single empowered agency (e.g., CISA, ENISA) improves coherence.
- Public–Private Collaboration: Mandated coordination between the government and private sector enhances threat response.
- Rights-Based Governance: Integration of cybersecurity with data protection and civil liberties ensures legitimacy and compliance.
- Cross-Border Engagement: Effective legal structures allow international collaboration and cyber diplomacy.

The importance of interoperability and global cooperation in cybersecurity governance . Countries that isolate their strategies from international frameworks are more vulnerable to transnational cyber threats—India being a case in point.

India can adopt several lessons from these comparative experiences:

- Establish a comprehensive cybersecurity law with well-defined enforcement mechanisms.
- Designate an apex cybersecurity agency with legal authority and operational autonomy.
- Harmonize cybersecurity policy with data protection and privacy frameworks.
- Institutionalize compliance protocols, sector-specific guidelines, and audit obligations.
- Develop international legal pathways to participate in cyber diplomacy and joint operations.

Without legal alignment and institutional cohesion, India's strategy will remain a "paper tiger." Comparative insights thus provide a roadmap for transforming India's cyber aspirations into tangible, enforceable governance.

The comparative analysis reveals that India must move beyond policy declarations and invest in statutory and institutional reform. Countries like the U.S., EU, and Pakistan have made cybersecurity a legislative and operational priority. To ensure that its National Cybersecurity Strategy achieves real-world impact, India must adopt a legally integrated, rights-

respecting, and globally connected approach rooted in the best practices of modern cyber governance.

Recommendations and Reform Proposals

To ensure the effective implementation of the National Cybersecurity Strategy (2020 draft), India must undertake a series of targeted legal, institutional, and policy reforms that bridge the gap between strategy and enforceability.

- The most urgent need is to enact a comprehensive cybersecurity law that codifies the principles outlined in the NCS 2020 and assigns clear legal duties to stakeholders across sectors. Such a law must move beyond the outdated IT Act, 2000, and incorporate contemporary threat environments, including AI-enabled attacks and critical infrastructure vulnerabilities .
- India should establish a centralized and autonomous cybersecurity authority with legislative backing. The current fragmentation between CERT-In, NCIIPC, and MeitY hampers coordination and response. A single nodal agency akin to the U.S. CISA could enhance operational efficiency and accountability .
- Cybersecurity regulation must be integrated with data protection and digital rights frameworks. Rights-respecting model where cybersecurity initiatives do not undermine privacy, due process, or free expression .
- India must institutionalize regular cybersecurity audits and compliance protocols, particularly in critical sectors. Codifying risk assessment mechanisms across public and private domains is key to proactive defense .
- Lastly, India should deepen international cooperation, aligning its legal frameworks with global cyber norms. The importance of treaties, joint task forces, and cyber diplomacy for a resilient, interconnected cyber defence architecture.

V. CONCLUSION

India's digital transformation has accelerated the need for a robust, enforceable, and future-ready cybersecurity framework. While the National Cybersecurity Strategy (2020 draft) offers a comprehensive policy vision, this study has demonstrated that it suffers from significant shortcomings in terms of legal enforceability, institutional coordination, and operational readiness.

The analysis reveals that the current legal regime, primarily governed by the Information Technology Act, 2000, is outdated and lacks provisions necessary to implement the strategy's goals. Sectoral regulations and institutional mandates remain fragmented and uncoordinated, undermining both efficiency and accountability. Moreover, the absence of a unified cybersecurity statute, and the failure to integrate cybersecurity with the Digital Personal Data Protection Act, 2023, leaves critical gaps in rights protection and data governance.

A comparative study of the United States, European Union, and Pakistan highlights how legislative codification, centralized oversight, privacy integration, and international cooperation have played pivotal roles in creating effective national cybersecurity models. These global best practices underscore the importance of embedding cybersecurity strategy within a clear legal framework.

To bridge the gap between policy and law, India must take decisive steps: legislate a comprehensive cybersecurity law, establish a central coordinating authority, harmonize legal frameworks, and align with global norms. These reforms are not only vital for enhancing national security but also for protecting democratic values and fostering trust in India's digital infrastructure.

Ultimately, cybersecurity in India must move from aspirational policy to enforceable law, only then can it meet the demands of a rapidly evolving digital age.

REFERENCE

1. YAGATI, A.K., Cybersecurity Legislation in India: A Comprehensive Review and Analysis, Cyber Crime &, p.78.
2. Kothiyal, S., The Critical Challenges of India's Cybersecurity Laws and Regulations, (2023) 5(1) Indian JL & Legal Rsch. 1.

3. Mishra, A. et al., Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations (2022) 120 Computers & Security 102820.
4. Saleem, B. et al., A Survey of Cybersecurity Laws, Regulations, and Policies in Technologically Advanced Nations (2024) 5(4) International Cybersecurity Law Review 533.
5. Singh, V. & Malik, V., Indian Cybersecurity Turf: A 2020 Position Paper (2021) 9(1) Journal of Network Security 42.
6. Singh, T.K., India's Cybersecurity Policy: Evolution and Trend Analyses, (2024) Taylor & Francis.
7. Kovacs, A., Cybersecurity and Data Protection Regulation in India, in CyberBRICS (2021) 133–181.
8. Callanan, C. et al., Enhancing Global Cybersecurity Cooperation: European and Indian Perspectives, (2022) Observer Research Foundation 1–29.
9. Tejpal, K. et al., Cybersecurity: Pressing Priority in India (2023) 11(2) Online J. of Distance Education & e-Learning 2052.
10. Halder, D. & Jaishankar, K., Cyber Governance and Data Protection in India, in Routledge Companion to Global Cyber-Security Strategy (2021) 337–348.