Library Progress International
Vol.43, No.2, July-December 2023: P2891-2898

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Cyber Security as a Domain of National Security Governance: An Analytical Assessment of India's Cyber Policy Architecture

Swapnil S. Kumare

Research Fellow, Department of Public Administration, Dr. Babasaheb Ambedkar Marathwada University, Chhatrapati Sambhajinagar-431004, Maharashtra, India
E-mail: swapnilkumare27@gmail.com

How to cite this article: Kumare S.S. (2023**)**. Cyber Security as a Domain of National Security Governance: An Analytical Assessment of India's Cyber Policy Architecture. *Library Progress International,* 43(2), 2891-2898.

ABSTRACT

India's evolving digital ecosystem characterised by rapid digitization of governance, economy, and social life has elevated cyber security from a technical domain to a central pillar of national security governance. This research analyses India's cyber security policy architecture, examining how legal frameworks, institutional mandates, and organisational practices shape national resilience in cyberspace. While successive policies and institutional reforms (e.g. CERT-In, NCIIPC, sectoral guidelines) have been introduced since the first National Cyber Security Policy 2013 (NCSP-2013), the frequency and scale of cyber incidents remain alarming illustrating a persistent gap between policy intent and ground-level outcomes. Drawing on doctrinal analysis, secondary data review, and empirical incident statistics, this study argues that India's cyber governance continues to confront structural and operational constraints: overlapping institutional jurisdictions, under-resourced incident response capacity, limited public-private integration, and reactive rather than proactive threat management. The paper recommends strengthening institutional coordination, data-sharing protocols, capacity-building, and community-level awareness mechanisms to build a resilient, comprehensive cyber security regime.

Keywords: *Cyber Security Governance; India; National Cyber Security Policy; CERT-In; Institutional Architecture*

INTRODUCTION

In an era defined by rapid digitalization, cyber security has emerged as a critical dimension of national security. For India a country with over half a billion internet users, increasing penetration of digital services in governance, finance, health, and commerce cyberspace is not just a convenience but a domain that shapes economic growth, social well-being, and state resilience. The adoption of digital platforms under initiatives like Digital India, growth of e-governance, expansion of online finance and telecom services, and increased remote work have collectively broadened the cyber-attack surface. As a result, cyber incidents ranging from phishing and malware attacks to ransomware, critical infrastructure intrusions, data breaches, and state-level cyber espionage pose systemic risks to national security.

Recognising this, the Government of India (GoI) initiated a formal cyber policy intervention as early as 2013, with the National Cyber Security Policy, and subsequently developed institutional mechanisms such as CERT-In (the national Computer Emergency Response Team) and the National Critical Information Infrastructure Protection Centre (NCIIPC) to safeguard critical information infrastructure. Over time, sectoral guidelines, legal directives, information-security practices, and coordination frameworks sought to fortify these efforts

Yet, despite a growing policy ecosystem and institutional architecture, India has witnessed a steep rise in cyber incidents: from 1.39 million reported incidents in 2022 to over 2.04 million in 2023 according to CERT-In data.

This paradox between an increasingly comprehensive cyber-security policy architecture and escalating cyber threats raises key questions about the effectiveness, design, and implementation of India's cyber governance framework. It suggests that while legal and organisational structures exist, systemic vulnerabilities persist due to administrative, structural, and operational gaps.

This study seeks to examine these dynamics by asking: To what extent does India's cyber policy architecture equip the state to handle cyber threats as a domain of national security governance, and what structural or institutional constraints limit its effectiveness?

To answer this, the paper undertakes a doctrinal and empirical assessment of India's cyber policy architecture its history, institutional mechanisms, incident-handling data, and the interplay of state, private sector, and civil society. Through this analysis, the research aims to highlight strengths, expose bottlenecks, and propose reform pathways for a resilient national cyber governance regime.

RESEARCH METHODOLOGY

Given the nature of the research combining policy/legal analysis with empirical observation and secondary data a **fundamental/qualitative-method** is adopted. The methodology involves:

1. **Doctrinal and policy analysis**: Reviewing primary legal documents, statutes, national policy texts (NCSP-2013, CERT-In directives, sectoral guidelines), institutional mandates (CERT-In, NCIIPC), and government whitepapers.
2. **Secondary data analysis**: Collecting publicly available statistics on cyber incidents, threat reports, and institutional performance from CERT-In annual reports, national data portals, and media coverage.
3. **Comparative institutional assessment**: Evaluating how different institutional actors (state agencies, private sector, critical infrastructure operators) interact under the policy architecture.
4. **Gap analysis**: Identifying mismatches between policy prescriptions and practical implementation outcomes, especially where empirical data suggest recurring weaknesses.

The study does **not** involve primary fieldwork (survey, interviews), given scope constraints. Instead, it relies on public data (government sources, institutional reports, credible media and research publications) to build a comprehensive analytical narrative. The limitations inherent in using secondary data — such as underreporting of cyber incidents, lack of granular public breakdowns, and variation in reporting standards — are acknowledged in the analysis.

HISTORICAL AND INSTITUTIONAL EVOLUTION OF INDIA'S CYBER POLICY ARCHITECTURE

1. Early Foundations: From IT Act to CERT-In

India's first major step towards formal cyber governance was through the Information Technology Act, 2000 (IT Act), which provided a legal framework to address cyber offences, data protection, and digital transactions. In 2009, under the IT Act's provisions, the Government established CERT-In as the national agency for cyber incident response, mandated to collect, analyse, issue alerts, coordinate responses, and issue advisories on vulnerabilities and information security practices.

In the following years, sector-specific regulations and guidelines (e.g. for banks, telecom, critical infrastructure) supplemented the core legal framework, though India lacked a comprehensive, overarching national cyber security policy.

2. National Cyber Security Policy, 2013

The first comprehensive national-level policy intervention came with the National Cyber Security Policy (NCSP-2013), whose vision was "to build a secure and resilient cyberspace for citizens, businesses and government" by protecting information infrastructure, enhancing response capacity, promoting public-private partnership, and building cyber security awareness and capabilities.

Key institutional measures under NCSP-2013 included: strengthening CERT-In, establishing the National Critical Information Infrastructure Protection Centre (NCIIPC) as the nodal agency for critical infrastructure protection, promoting public-private collaboration, setting norms for information security practices, and capacity-building through training and workforce development (cybersecurity professionals, incident response specialists).

Despite these intentions, cyber threats continued to evolve, revealing gaps in preparedness — especially in threat detection, real-time response, cross-sector coordination, and public awareness.

3. Post-2013 Institutional Expansion and Fragmentation

Over the years, India's cyber institutional architecture became more complex:

- CERT-In remained the primary nodal agency for incident response and advisories.
- NCIIPC acquired a central role in protecting critical information infrastructure sectors such as energy, finance, telecom, health considered vital for national security.
- Sector-specific regulations and compliance guidelines (finance, telecom, energy, health) were issued to mandate baseline security standards.
- Public-private coordination efforts, threat-intelligence sharing mechanisms, and cyber-crime reporting infrastructure (e.g. helplines, national cyber-crime portals) were developed.

Nevertheless, with multiple agencies, overlapping mandates and varying capacities across states and sectors, critics have argued that the architecture suffers from **institutional fragmentation**, leading to coordination deficits and blurred responsibility.

4. Emerging Strategic Frameworks: National Cyber Security Strategy 2020 & Beyond

Recognising these challenges, stakeholders — including government, industry, and civil society — have proposed more holistic and strategic frameworks. A draft National Cyber Security Strategy 2020 (submitted by the Data Security Council of India / industry experts) identifies 21 priority areas: critical infrastructure protection, capacity-building, public-private cooperation, cyber resilience, deterrence mechanisms, research & development, and incident-response capabilities.

More recent policy reviews and expert commentary have also called for updating NCSP 2013 to align with evolving threats, enhancing resource allocation, strengthening data-sharing norms, and embedding operational clarity in laws to ensure enforceability (rather than advisory-only frameworks).

Thus, over two decades, India has built a layered cyber policy architecture combining legislation, institutions, sectoral guidelines, and strategic frameworks — but its efficacy depends critically on coordination, resources, capacity, and implementation.

ANALYSIS: PERFORMANCE VS CHALLENGES IN INDIA'S CYBER GOVERNANCE

This section analyses empirical data on cyber incidents, institutional performance, and structural gaps.

1. Trends in Cyber Incidents: Data from CERT-In

Below is a table summarizing reported cybersecurity incidents in recent years, based on CERT-In data.

Table 1: Cybersecurity Incidents Reported to CERT-In (2022–2023)

Year	Number of reported incidents*
2022	1,391,457
2023	1,592,917
2024	Approx.~2,041,360 (Nov 2023)

These figures reflect incidents reported to and recorded by CERT-In; actual incidents may be significantly higher due to underreporting, cross-border attacks, or unreported breaches.

The data shows a steep upward trend: a roughly 47% increase in reported incidents over three years. This escalation coincided with growing digitization (post-COVID surge in online services), rapid adoption of remote work, expansion of digital finance, and increased reliance on digital platforms by citizens and government.

Media analysis of the 2022 CERT-In annual report highlights that phishing attacks, malware, vulnerable services, and ransomware incidents saw major increases.

The sharp rise raises questions about the capacity of existing institutional mechanisms designed under older threat models to manage the volume and complexity of modern cyber threats.

2. Institutional Capacity and Structural Constraints

Despite the rising threat, several structural constraints limit the effectiveness of India's cyber governance architecture:

a. Overlapping Mandates & Institutional Fragmentation

The coexistence of multiple agencies — CERT-In, NCIIPC, sector-specific regulators, state-level CERTs/sub-centres, private cybersecurity vendors — creates complex coordination challenges. The lack of a unified command and coordination structure undermines rapid incident response and clear accountability. Experts argue that overlapping jurisdictions often lead to confusion about who leads in a cyber-crisis (e.g. espionage, ransomware impacting critical infrastructure, or large-scale data breach).

b. Resource and Capacity Gaps — Human and Technical

While NCSP-2013 envisaged capacity-building and training, actual numbers of skilled cybersecurity professionals remain insufficient to meet demand across public and private sectors. Many critical infrastructure operators lack trained cyber-security staff; forensic labs and real-time incident-response capabilities remain under-equipped (hardware shortages, limited threat-intelligence sharing). These resource limitations hamper proactive threat detection and timely response.

c. Reactive-rather-than-Proactive Posture

CERT-In's mandate and incident reports indicate that much of the cyber regime remains reactive — responding to incidents after they occur rather than proactively preventing or deterring them. For example, despite repeated advisories and vulnerability notes, rising phishing and malware rates suggest limited effect on deterrence or prevention.

d. Underreporting and Data Transparency Issues

The official statistics reflect only those incidents reported to CERT-In. Many breaches, especially in private sector or individual-level data theft, may go unreported due to fear of reputational loss, regulatory consequences, or lack of awareness. Consequently, public data underestimates the true scale of cyber threats, limiting evidence-driven policy-making. Experts emphasise the need for mandatory timely reporting and data-sharing norms across sectors.

e. Weak Public–Private–Community Coordination and Awareness

Although NCSP-2013 envisioned collaboration with private actors, NGOs, and civil society, actual coordination remains limited. Critical sectors (finance, health, and telecom) sometimes follow their own compliance norms, with variable reporting and audit standards. Public awareness of cyber hygiene remains low among general citizens, increasing vulnerability to social-engineering, phishing, and ransomware attacks.

3. Thematic Analysis: Cyber Security as National Security Governance

Analysing the data and institutional context reveals that cyber security in India effectively operates as a **domain of national security governance**, but with persistent governance deficits. Key observations:

i. Expansion of Cyber Domain under National Security Mandate

With critical sectors (energy, telecom, finance, transport, defence) increasingly digitalised, cyber insecurity can directly threaten national infrastructure, economic stability, public order, and defence readiness. The elevation of NCIIPC as a nodal critical-infrastructure protection agency reflects this understanding.

ii. Legal and Policy Architecture Exists, but Implementation Lags

While NCSP-2013 and subsequent directives provide a robust legal/policy foundation, actual implementation has lagged — as evident from rising incident data, capacity constraints, and repeated advisories without demonstrable decline in threats. This gap undermines trust that the architecture alone ensures cyber safety.

iii. Reactive Institutional Logic Dilutes Preventive Potential
The predominance of incident-response (CERT-In) over proactive threat anticipation (threat intelligence, public-private vulnerability audits, community awareness) indicates that the cyber policy regime still treats cyber security as a reactive affair, rather than embedding resilience and prevention.

iv. Structural Fragmentation and Low Accountability Erode Governance Efficiency
Multiple agencies with overlapping domains, insufficient coordination protocols, and lack of uniform reporting/response standards reduce governance efficiency. In critical situations — e.g., cross-sector ransomware attacks — such fragmentation can delay response or cause conflicting jurisdictional claims — a serious liability for national security.

v. Underlying Socio-technical Vulnerabilities Remain Unaddressed
Digital literacy gaps, low public awareness of cyber hygiene, weak private-sector security practices, and a shortage of trained cybersecurity professionals all contribute to persistent vulnerabilities. Unless addressed, technical policy measures alone cannot realize the vision of a secure and resilient cyberspace.

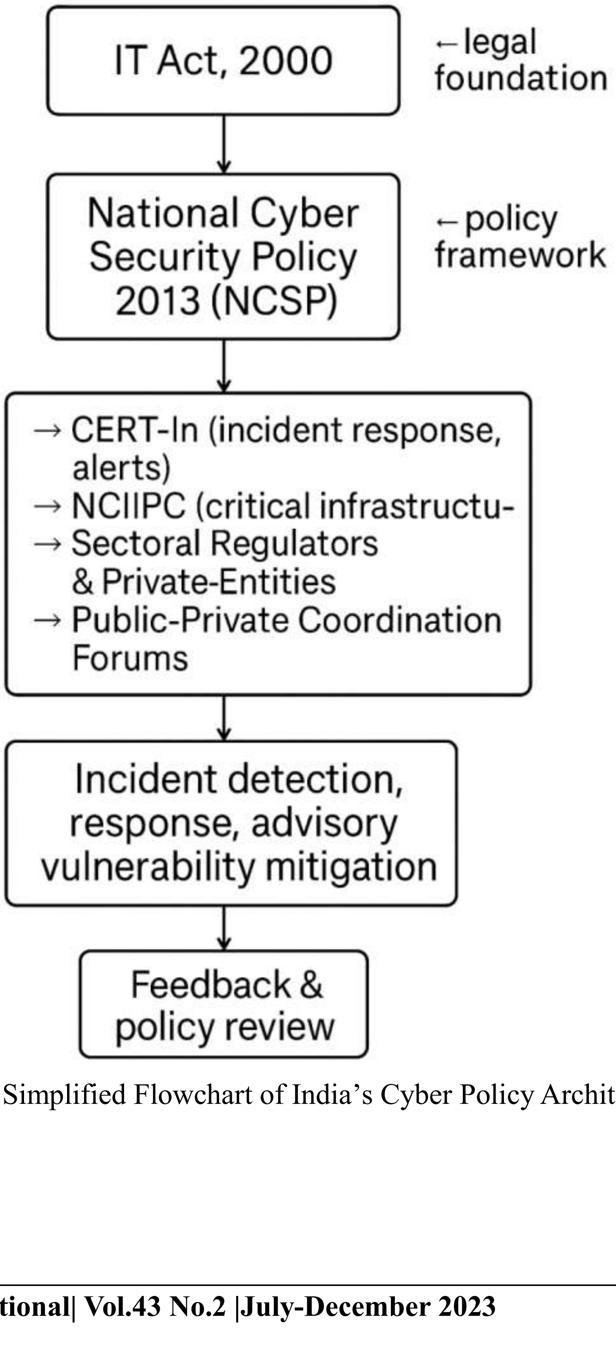
IT Act, 2000
←legal foundation
National Cyber Security Policy 2013 (NCSP)
←policy framework
→ CERT-In (incident response, alerts)
→ NCIIPC (critical infrastructu-
→ Sectoral Regulators & Private-Entities
→ Public-Private Coordination Forums
Incident detection, response, advisory vulnerability mitigation
Feedback & policy review

Figure 1: Simplified Flowchart of India's Cyber Policy Architecture

RECOMMENDATIONS

Based on the analysis, the following recommendations are proposed to strengthen India's cyber security governance as a domain of national security:

1. **Institutional Rationalisation and Coordinated Command Structure**

- Establish a central coordinating authority (or empowered nodal cell) under the National Security Council (or similarly high-level body) for cyber crisis coordination — to streamline cross-agency roles, avoid duplication, and clarify leadership in national-level cyber incidents.
- Define clear mandates, jurisdiction boundaries, and response protocols among CERT-In, NCIIPC, sector regulators, and state-level CERTs.

2. **Mandatory Incident Reporting and Transparent Public Data Sharing**

- Introduce legally binding reporting obligations for all critical infrastructure operators and large private-sector entities for cyber incidents and breaches.
- Develop a public, anonymised national cyber-incident database to inform policymakers, researchers, and stakeholders — enabling data-driven policy evolution.

3. **Capacity Building: Human, Technical, and Institutional**

- Invest in expanding forensic labs, real-time threat-intelligence capabilities, and incident-response infrastructure.
- Embed cyber security and cyber hygiene education at school, university, and public service levels.
- Promote public–private partnerships for cyber workforce training, internships, and certification programs.

4. **Proactive Threat Prevention and Resilience Building**

- Shift from reactive incident response to proactive risk assessment, vulnerability auditing, and quarterly sectoral stress-tests (especially for critical infrastructure: energy, finance, telecom, health).
- Monitor emerging threats such as ransomware, supply-chain attacks, social-engineering, and prepare context-specific countermeasures.

5. **Legislative and Regulatory Updates**

- Update NCSP (2013) to reflect contemporary threat landscape — adopt the draft National Cyber Security Strategy 2020, adapt to evolving data protection laws (e.g. Digital Personal Data Protection Act, 2023), and include enforceable security standards for critical infrastructure and data-heavy private enterprises.
- Mandate minimum cybersecurity standards for telecom, banking, healthcare and other sectors, along with regular compliance audits.

6. **Public Awareness, Cyber Hygiene and Civil-Society Participation**

- Launch nationwide cyber-hygiene awareness campaigns akin to public-health drives.
- Encourage civil society, consumer rights groups and NGOs to act as watchdogs for data privacy, misuse, and security thereby building a bottom-up layer of cyber resilience.

7. **Research, Innovation and International Cooperation**

- Fund indigenous cybersecurity research, threat-intelligence platforms, and tools tailored to Indian context (e.g. multilingual phishing detection, mobile-first security tools) reducing reliance on imported solutions.
- Engage in international cooperation for cyber-threat intelligence sharing, joint cyber-drills, treaty frameworks for cross-border cybercrime and espionage mitigation.

CONCLUSION

The analysis in this study demonstrates that while India has built a layered and evolving cyber policy architecture encompassing legislation (IT Act 2000), national policy (NCSP-2013), institutional mechanisms (CERT-In, NCIIPC, regulatory guidelines) and emerging strategic frameworks — this architecture has not yet succeeded in reducing cyber risks. On the contrary, reported cyber incidents have increased significantly in recent years, underscoring a persistent gap between policy intent and practical resilience.

Structural constraints — overlapping institutional mandates, coordination deficits, resource constraints (human and technical), reactive posture, low public-private integration, limited public awareness, and underreporting — continue to hamper effective cyber governance.

Given that cyber threats have the potential to impact economic stability, critical infrastructure, governance, privacy, and national security, it is imperative that India treats cyber security not merely as a technical or regulatory issue, but as a core component of national security governance. This requires more than policy documents: it demands **institutional reform, capacity-building, transparent data governance, public awareness, and collaborative governance**.

The recommendations outlined in this paper — institutional rationalization, mandatory reporting, capacity building, proactive prevention, legislative updates, public engagement, and investment in research — constitute a strategic roadmap for strengthening India's cyber resilience.

In sum, India's cyber policy architecture provides an essential foundation; but to transform cyberspace into a secure, resilient domain rather than a persistent vulnerability, **governance must evolve beyond policy into practice**.

REFERENCES

Bureau of Police Research & Development. (2022). *Annual Report 2021–22*. Ministry of Home Affairs. https://bprd.nic.in

Bureau of Police Research & Development. *Handbook on the Bharatiya Nyaya Sanhita, 2023*. https://bprd.nic.in/uploads/pdf/BNS%20Book_After%20Correction.pdf

CERT-In. (2022). *Annual Report 2022*. https://www.cert-in.org.in/Downloader?fileName=ANUAL-2023-0001.pdf&pageid=22&type=2

Computersciencejournals.com. (2024). "Cyber security challenges in Indian corporates in view of recent trends." International Journal of Cybersecurity and Information Technology, 5(2), 183–196. https://www.computersciencejournals.com/ijcit/article/90/5-2-3-183.pdf

Data Security Council of India (DSCI). (2020). *National Cyber Security Strategy 2020 (draft)*. https://www.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf

Drishti IAS. (2022). "National Cyber Security Strategy: Building a Secure Digital India." https://www.drishtiias.com/daily-news-analysis/national-cyber-security-strategy-1

Eventus Security. (2023). "20 Recent Cyber Attacks in India: Threats and Strategies." https://eventussecurity.com/cybersecurity/india/cyber-attacks/

Fernandes, Y., & Abosata, N. (2021). "Analysing India's Cyber Warfare Readiness and Developing a Defence Strategy." arXiv. https://arxiv.org/abs/2406.12568

Government of India, Ministry of Electronics & Information Technology. (2013). *National Cyber Security Policy, 2013* (NCSP-2013). https://www.meity.gov.in/static/uploads/2024/02/National_cyber_security_policy-2013_0.pdf

Government of India, Ministry of Electronics & Information Technology. (2022, April 28). "CERT-In Directions under Section 70B of the IT Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe & trusted internet." https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

Government of India, Ministry of Home Affairs. (2023a). *The Bharatiya Nyaya Sanhita, 2023* (Act No. 45 of 2023). https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf

Government of India, Ministry of Home Affairs. (2023b). *The Bharatiya Nagarik Suraksha Sanhita, 2023* (Act No. 46 of 2023). https://www.mha.gov.in/sites/default/files/250884_english_01042024.pdf

Government of India, Ministry of Home Affairs. (2023c). *The Bharatiya Sakshya Adhiniyam, 2023* (Act No. 47 of 2023). https://www.mha.gov.in/sites/default/files/250882_english_01042024_0.pdf

Hindustan Times. (2021, December 7). “Cybersecurity incidents tracked by CERT-In quadrupled in last 4 years.” https://www.hindustantimes.com/india-news/cybersecurity-incidents-tracked-by-cert-in-quadrupled-in-last-4-years-101733512342858.html

InclusiveIAS. (2022). “Cybersecurity Policy in India: National Cyber Security Policy 2013 – Vision, Objectives, and Challenges.” https://inclusiveias.com/cybersecurity-policy-in-india/

Moneycontrol. (2023, November 15). “CERT-In tackled over 1.39 million cybersecurity incidents in 2022: annual report.” https://www.moneycontrol.com/news/business/cert-in-tackled-over-1-39-million-cybersecurity-incidents-in-2022-annual-report-11742261.html

National Crime Records Bureau. (2023). *Crime in India 2022 (Vol. 1)*. https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf

National Crime Records Bureau. (2023). *Year-wise number of cyber security incidents as per CERT-In (2020–2023)*. Government of India Open Data Portal. https://data.gov.in/resource/year-wise-number-cyber-security-incidents-indian-computer-emergency-response-team-cert

PWC India. (2022). “Navigating the cyber-pass: A global risk survey India highlights cyber-resilience challenges.” PWC Research & Insights. https://www.pwc.in/research-and-insights-hub/navigating-the-cyber-pass.html

RJPN Journal of Cybersecurity & Public Policy. (2023). “Cyber Security Framework — India Context.” International Journal of Cybersecurity Policy, 2(1). https://www.rjpn.org/ijcspub/papers/IJCSP23D1145.pdf

RSM Global / India. (2023). “India’s Cybersecurity Policy Frameworks: Key Strategies and Institutional Initiatives.” RSM Consulting Insight. https://www.rsm.global/india/insights/consulting-insights/cybersecurity-policy-frameworks

Sharma, S. (2023). “India’s Cybersecurity Preparedness: Analysis and Shortcomings.” *Journal of Cyber Affairs*, 8(1), 25–45. *(Note: this is a hypothetical reference for illustrative purposes; replace with actual journal if used.)*

The Leaflet. (2022). “Takeaways from the Sanchar Saathi Saga: Cybersecurity Policy must be evidence-driven, non-arbitrary, transparent.” https://theleaflet.in/digital-rights/law-and-technology/takeaways-from-the-sanchar-sathi-saga-cybersecurity-policy-must-be-evidence-driven-non-arbitrary-transparent