International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cybersecurity, Digital Governance, and National Security: Emerging Challenges and Policy Responses in India

Ritesh Kumar Panda

Independent Research Scholar, M.Sc. in Computer Science, Sambalpur University, Odisha, India

Abstract:
This paper studies how cyber security, digital governance, and national security are connected in India. It looks on three things. The new laws and institutions made by government, and the gap between policy and real implementation and the changing cyber threats. Now a days India's cyber -attack risk has increased a lot. because, digital India and fast development of digital public infrastructure. According to official documents and research from 2013 to 2025, the paper shows India's journey from the IT act of 2000 to the digital personal data protection act 2023, The national cybersecurity framework 2024, and the Telecom cyber security rules 2024. In order to improve India's cyber resilience while upholding democratic governance principles, the research highlights three major issues: the geopolitics of data sovereignty, the fragmented regulatory architecture, and the conflict between civil liberties and state monitoring. Scholars, decision-makers, and security specialists addressing the new governance issues of digitally networked countries in the Global South should evaluate the findings.

Keywords: Cybersecurity; Digital Governance; National Security; India; CERT-In; DPDP Act; Data sovereignty; Critical information infrastructure; Policy

1. Introduction:

Threats to national security have significantly changed in the twenty-first century. States now have to deal with enemies that operate in the unseen realm of cyberspace in addition to traditional military and geopolitical threats. These adversaries have the power to harm vital infrastructure, steal personal information, disseminate misleading information, and jeopardize democratic institutions (Nye, 2017). It has a significant impact on India, the largest populous democracy in the world and one of the fastest-growing digital economies. The nation boasts the world's largest biometric identity system (Aadhaar), over 881 million internet users (Ericsson, 2024), and a digital public infrastructure known as the "India Stack" that handles billions of financial transactions per month. However, because of this digital depth, a successful large-scale cyberattack might have an impact on a number of industries that are vital to the general welfare, including energy, transportation, defence, banking, and health. The data presents a dismal image. Over 2.26 million cybersecurity incidents were reported by the Indian Computer Emergency Response Team (CERT-In) in 2024, more than twice as many as the 1.03 million reported in 2022 (PIB, 2024). Data breaches cost the nation more than USD 2.18 million in 2023, according to the Reserve Bank of India, a 28% increase over the preceding three years (Carnegie Endowment, 2025). Cyberattacks against Indian government systems rose by 138% between 2019 and 2023 (Carnegie Endowment, 2025). In the

meantime, during the fiscal year 2024–2025 alone, the Data Security Council of India (DSCI) recorded 369 million malware detections across 8.44 million endpoints, with an average of 702 possible attacks per minute (6clicks, 2025).

In response, India has put in place a number of institutional, legal, and regulatory safeguards. The National Cybersecurity Reference Framework (NCRF) was published in 2024, the Telecommunications (Telecom Cyber Security) Rules were published in November 2024, and the Digital Personal Data Protection Act (DPDPA) was passed in August 2023. After making notable advancements in the legal, technological, capacity-building, and cooperation aspects of cyber governance, India was ranked Tier 1 in the International Telecommunication Union's (ITU) Global Cybersecurity Index that year (Carnegie Endowment, 2025). The ITU did, however, also note that India's organizational cybersecurity measures needed to be strengthened, implying that achieving policy goals requires a robust institutional framework.

This document is organized as follows. Section 2 reviews the theoretical literature on digital governance and cybersecurity. Section 3 shows how India's institutional and regulatory framework for cybersecurity has evolved. Section 4 looks at the current state of threat. Section 5 looks at three key governance challenges. Section 6 evaluates India's policy responses. Section 7 offers recommendations. Section 8 concludes.

2. Theoretical Framework: Cybersecurity, Governance, and National Security:

From being a specialized technical study focused on network security, cybersecurity studies have developed into a multidisciplinary field that includes public administration, law, political science, and international relations. An early paradigm for understanding security as a speech act—a process by which threats are "securitized" by political actors—was provided by academics such as Buzan, Waever, and De Wilde (1998). This viewpoint has been applied by later researchers to study cyberspace, looking at how governments create cyberthreats to facilitate enormous surveillance and regulatory power (Cavelty, 2014). Hansen and Nissenbaum (2009) made a distinction between "hyper securitization"—the propensity to characterize all cyber dangers in terms of catastrophic scenarios—and a more nuanced understanding of frequent cyber flaws. This dichotomy is evident in Indian policymaking, which alternates between long-term governance-building exercises and emergency responses to high-profile catastrophes. Digital governance" describes the use of information and communication technology (ICT) for state authority, economic activity control, and public service delivery. There are many different ways to think about this topic, from participatory e-democracy to authoritarian digital control (Deibert, 2013).

India's digital public infrastructure truly democratizes access to services for hundreds of millions of people, but the nation's surveillance apparatus—which includes the Centralized Monitoring System (CMS) and the legal powers granted by Sections 69 and 69A of the Information Technology Act—raises serious concerns about civil liberties (Internet Governance Project, 2024). The multi-actor nature of cyberspace makes national security in the cyber domain more challenging Unlike traditional security threats, which are often state-to-state, cyber hazards can originate from state actors, non-state entities (such as hacktivists and criminal organizations), or hybrid actors that lie somewhere in between (Rid & Buchanan, 2015). The difficulty of precisely determining the origin of a cyberattack, known as the attribution problem, makes it difficult to use conventional deterrent techniques and gives opponents plausible deniability. This problem is made worse by India's antagonistic relations with its neighbours, especially China and Pakistan.

Now a days cyber threats are not only limited in websites or personal data but also it targets the real infra-

structure. A key example of cyber risk in India was the October 2020 attack on Mumbai's electrical infrastructure. According to sources it was found that it was linked to Chinese state-sponsored hackers (Recorded Future, 2021). Finally, a critical foundation for understanding the debates surrounding data localization in India is provided by the literature on digital geopolitics and data sovereignty (Jiang et al., 2024). Data is increasingly treated as a "new oil". Whoever has data has power, money, intelligence and everything. He can do anything. India is a middle-powered country. On one hand, it wants data to flow freely so that business can grow. On the other hand, it wants data from essential services like banking and healthcare to be stored in India so that it is safe for everyone (TechPolicy). Press, 2025).

3. The Evolution of India's Cybersecurity Legislative and Institutional Landscape:

3.1 The Information Technology Act, 2000 and Its Amendments

The Information Technology Act,2000(IT Act), India's first law to oppose cybercrime and govern electronic trade, is the source of country's cybersecurity regulatory framework. The IT Act forbids the dissemination of porn, hacking, data theft, and confidentiality crimes. It also established the Cyber Regulations Appellate Tribunal (CRAT) (CSIC, 2024). However, the original Act's scope was constrained, and it was unable to sufficiently account for the complexity of newly emerging cyberthreats. Information Technology Amendment Act, 2008 greatly expanded the framework by defining and punishing identity theft and phishing, adding provisions on cyberterrorism (Section 66F), granting the government the power to monitor, intercept, or block information in the interest of national security (Sections 69, 69A, and 69B), and designating particular computer resources as "protected systems" under Section 70 (UpGuard, 2025). Section 70A permitted the establishment of the National Critical Information Infrastructure Protection Centre (NCIIPC), while Section 70B created the Indian Computer Emergency Response Team (CERT-In) as the national organization for cybersecurity incident response. Although it is growing out of date, India's fundamental cybersecurity statute is still the IT Act. Provisions created in the early 2000s, according to critics, are inadequate to handle modern threats such supply chain attacks, ransomware, misleading information generated by artificial intelligence, and vulnerabilities in cloud and Internet of Things (IoT) environments (Padhai.ai, 2026). A comprehensive, stand-alone Cybersecurity Act that updates and unifies the current disjointed framework has been demanded by a number of legislative committees.

3.2 The Digital Personal Data Protection Act, 2023

After more than two decades of deliberation, India passed the Digital Personal Data Protection Act (DPDPA) on August 11, 2023. The Act creates rights for "data principals" (individuals whose data is processed) and obligations for "data fiduciaries" (entities that process data). It is based on concepts similar to but very different from the General Data Protection Regulation (GDPR) of the European Union (UpGuard, 2025). Notably, detractors claim that the DPDPA's broad exclusions for national security and law enforcement could be misused to undermine data privacy laws (Jiang et al., 2024). n order to ease trade with important partners like the United States and Japan, the Act loosens the strong data localization requirements found in previous draft versions and permits cross-border data transfers subject to government-notified constraints (Jiang et al., 2024). In January 2025, the Ministry of Electronics and Information Technology (MeitY) published suggested implementation guidelines. These rules have been criticized for having too much executive discretion and for being unclear about security and privacy protections (TechPolicy.Press, 2025b).

3.3 The National Cybersecurity Reference Framework and Telecom Cyber Security Rules, 2024

India published the National Cybersecurity Reference Framework (NCRF) in 2024. This important policy document, which aims to offer a thorough road map for protecting the nation's digital ecosystem, is overseen by the National Cybersecurity Coordinator (Carnegie Endowment, 2025). The NCRF aims to coordinate efforts between government ministries and the business sector by addressing governance, risk management, incident response, and capacity building. The Department of Telecommunications (DoT) released the Telecommunications (Telecom Cyber Security) Rules, 2024 in May 2024 in response to proven assaults on Bharat Sanchar Nigam Limited (BSNL). These rules provide telecom operators with criteria for data acquisition, security precautions, and incident reporting (Carnegie Endowment, 2025). Furthermore, the DoT released the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024, which grant the government the power to classify any telecommunications network as Critical Telecommunication Infrastructure if its disruption would seriously harm the economy, public health, safety, or national security (Chambers and Partners, 2025).

3.4 Institutional Architecture

Despite accusations that it lacks uniformity and coordination, India's cybersecurity institutional architecture is multi-layered. Among the significant organizations area the CERT-In program of the Ministry of Electronics and Information Technology; (ii) the NCIIPC program of the National Technical Research Organization (NTRO) and the Prime Minister's Office (PMO); and (iii) the Indian Cyber Crime Coordination Centre (I4C) of the Ministry of Home Affairs, which oversees the National Cyber Crime Reporting Portal (cybercrime.gov.in) and coordinates law enforcement's responses to cybercrime (PIB, 2024b). (v) industry-specific regulators, such as the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), and the Insurance Regulatory and Development Authority (IRDAI), that have released their own cybersecurity frameworks for their respective sectors; and (iv) the National Cybersecurity Coordinator of the PMO, who oversees policy development and interagency coordination (Cyber law consulting, 2024).

4. The Current Cyber Threat Landscape in India:

4.1 Ransomware and Malware

One of the most disruptive cyberthreats that India is now confronting is ransomware. The All-India Institute of Medical Sciences (AIIMS) in New Delhi experienced a ransomware attack in October 2022 that rendered the hospital's digital systems inoperable for over a week, interfering with patient care, appointment scheduling, and billing while highlighting the vital health infrastructure's acute vulnerability to cyber threats (WebAsha, 2025). The extent and ubiquity of the danger were generally demonstrated by the DSCI's India Cyber danger Report 2025 for the fiscal year 2024–2025, which revealed 369 million malware detections over 8.44 million endpoints (6clicks, 2025). Artificial intelligence is increasingly being used by criminal organizations and state-sponsored organizations to produce malware that is flexible and can swiftly evade traditional defences (6clicks, 2025).

4.2 State-Sponsored and Advanced Persistent Threats

India is still at risk from state-sponsored advanced persistent threat (APT) actors. Red Echo, a Chinese state-sponsored outfit that purportedly pre-positioned malware in at least twelve Indian power sector companies, was linked by cybersecurity firm Recorded Future to the October 2020 Mumbai power outage (Recorded Future, 2021). The 2024 BSNL attack served as more evidence of the fragility of state-owned telecom infrastructure. Citing data security and national security concerns, the Indian government

gradually blocked hundreds of Chinese-related mobile applications after the 2020 Galwan Valley conflicts with China. As a result, these dangers became more geopolitical (Chambers and Partners, 2025). India's internet is currently the second most targeted in the world, according to the Carnegie Endowment (2025).

4.3 Disinformation and AI-Enabled Threats

The increasing danger of false information produced by AI was made clear during the general elections in India in 2024. To disseminate false information and sway public opinion, deepfake films, AI-generated voice impersonations of political personalities, and automated social media campaigns were employed (CIGI, 2024). AI and cyber operations present a fundamentally new challenge: generative AI lowers the cost of creating convincing fabrications to almost zero, whereas classic disinformation campaigns required substantial human effort to generate and spread. Finding and combating AI-generated false information is a significant governance challenge for a nation with 881 million internet users dispersed across multiple linguistic and geographic contexts.

4.4 Supply Chain and Telecom Infrastructure Threats

India was made aware of the susceptibility of telecom supply chains to state-sponsored infiltration by the multinational Salt Typhoon espionage operation, which compromised AT&T and Verizon's US communication networks (Carnegie Endowment, 2025). India's telecom infrastructure has also been impacted by cyberattacks, and the May 2024 BSNL intrusion demonstrated how crucial it is to preserve robust supply chain security protocols. In critical industries, where digital control systems now manage physical infrastructure such as power grids, transportation networks, and water treatment facilities, the convergence of information technology (IT) and operational technology (OT) has greatly expanded the attack surface (6clicks, 2025).5. Key Governance Challenges

4.5 Fragmented Regulatory Architecture and Coordination Deficits

The largest challenge to India's cybersecurity governance may be the split of regulatory authority across many ministries, agencies, and sectoral authorities. According to the Centre for International Governance Innovation (CIGI), "incoherent and uncoordinated regulations, at times promulgated without adequate consultation, may create confusion rather than certainty" (CIGI, 2024). One particular example of this problem is the difference in incident reporting deadlines: the CERT-In Directions of 2022 mandate reporting within six hours of a cyber incident, whereas the draft Telecommunications Critical Infrastructure Rules of 2024 impose a two-hour reporting window (CIGI, 2024). Organizations may be faced with three distinct and sometimes contradictory reporting requirements when the DPDPA's reporting duties take effect. To eliminate coordination gaps, the Parliamentary Standing Committee on Finance's 59th Report (July 2023) suggested creating a centralized cybersecurity regulatory body (NASSCOM, 2025). A centralized coordinating mechanism is linked to more effective national cyber resilience, according to comparative experience from the United States (Office of the National Cyber Director, established 2021), the European Union (Joint Cyber Unit), Singapore (updated Cybersecurity Strategy, 2021), and Japan (major institutional reforms since 2018) (NASSCOM, 2025).

4.6 Surveillance, Civil Liberties, and the Tension Between Security and Privacy

Under the guise of security, public order, or sovereignty, India's national security framework gives authorities extensive power to block internet material and intercept conversations. In the absence of strong procedural safeguards or independent judicial review, the central government may order the interception, monitoring, or blockage of information under Sections 69 and 69A of the IT Act. In May 2023, the Jammu and Kashmir government outlawed 14 free and open-source messaging apps on the grounds that terrorist communications were being supported by their end-to-end (E2E) encryption capabilities (Internet

Governance Project, 2024). According to the Internet Governance Project, which tracked India's "evolving assaults on private communications," E2E encryption is inherently at odds with both governmental security goals and individual privacy (Internet Governance Project, 2024). Additionally, the DPDPA has come under fire for giving the federal government extensive exclusions for national security reasons, which could essentially void a number of people's rights to data privacy. Scholars have seen a significant move towards authoritarianism in the Modi government's use of digital platforms, including as the dissemination of Hindu nationalist narratives to justify surveillance and content control (Jiang et al., 2024). Striking a balance between security requirements and civil rights guarantees is not just a technical or legal exercise; it is essentially an issue of democratic governance and the rule of law.

4.7 Data Sovereignty, Localisation, and Digital Geopolitics

India's approach to data sovereignty is shaped by the realization that data is a site of geopolitical contestation, a security resource, and an economic asset. With its digital economy contributing USD 500 billion to GDP and projected to reach USD 1 trillion by 2030, India has substantial financial incentives to encourage cross-border data flows (Rau's IAS, 2025). The concentration of Indian consumer data on foreign, primarily American, cloud and platform infrastructure also raise concerns about surveillance, economic reliance, and the capacity of foreign governments to get Indian data under local legal frameworks (TechPolicy, Press, 2025). In an attempt to manage this tension, the DPDPA permits cross-border data transfers while allowing the government to restrict flows to particular countries; SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF) of 2024 mandates data localization for "Regulatory Data"; and RBI has long maintained sectoral localization requirements for payment data (Global Data Alliance, 2025). The January 2025 Draft Rules, according to critics, are a data localization framework with "excessive executive discretion" and insufficient privacy measures (TechPolicy). Press, 2025b). The geopolitical aspect of data governance is further complicated by India's trade negotiations with the United States, which led to the removal of the 6% equalization levy on digital advertising in early 2025 as a result of pressure from the US (Tec Policy). This highlights external constraints on India's regulatory autonomy.Press, 2025).

5. Evaluating India's Policy Responses

5.1 Strengths

Over the last ten years, India’s government has made great progress in cybersecurity. After 25 years of discussion, the DPDPA which offers a fundamental framework for data protection was passed. In April 2022, CERT-In issued new cyber security directions requiring clock synchronization, required incident reporting and log retention across sectors (PIB, 2024). In 2024-25, CERT-In conducted 10,000 audits in critical sectors like banking, transport, and power to ensure that the system is secure (6clicks, 2025). The 14C and the National cyber crime Reporting portal have made it easier for citizen to report cybercrime. Anyone can now easily report online fraud or cyber-crime. India has been ranked Tier 1 in the ITU Global cybersecurity index 2024.This means that the world is recognizing that India is leading in the cyber security index.

India's cybersecurity government has advanced significantly in the past ten years. The DPDPA, which provides a basic foundation for data protection, was passed after 25 years of debate. Clock synchronization standards, mandatory incident reporting requirements, and cross-sector log retention responsibilities were implemented by CERT-In's April 2022 Cyber Security Directions (PIB, 2024). During the fiscal year 2024–2025, CERT-In conducted about 10,000 audits in critical areas like banking, transportation, and

power (6clicks, 2025). Citizens can now report cybercrime more easily thanks to the I4C and the National Cyber Crime Reporting Portal. India's Tier 1 status in the ITU Global Cybersecurity Index 2024. The Cowin vaccination platform powered financial inclusion and digital India program are illustration of successful digital governance.

5.2 Persistent Gaps

Even with these achievements, persistent vulnerabilities undermine India's cyber resilience. Instead of a single, separate cyber security act, Indi's governance is composed on sector specific regulations. presidential directives and an IT act 2000.This patchwork overlaps rules, makes compliance more difficult, and allows shrewd opponents to engage in regulatory arbitrage (Padhai.ai, 2026). The goal of the 2013 National Cyber security policy was to produce 500,000 cyber security experts in five years. That target was not met. Even today, there is a huge shortage of experts (CIGI, 2024). India's digital sovereignty and strategic autonomy are weakened by its dependence on foreign clouds and platforms like Google, AWS, Microsoft. There is no strong Indian alternative (NextIAS, 2025).

Earlier, IT and OT systems were separate. Now they have merged. Therefore, the risk of attacks on sectors like power grid and train has increased and the old security rules cannot handle it (6clicks, 2025).

The DPDPA and the IT act give the government a lot of power in surveillance and there are also some exemptions to which civil liberties i.e. the rights of the people, are neglected in the name of security.

6. Policy Recommendations:

In view of the previously mentioned facts, the report offers the following evidence-based recommendations for enhancing cybersecurity governance in India.

India should first pass a robust, independent cybersecurity act. Now we have the old IT act of 2000. It cannot cover the threats of today like ransomware, AI attack, supply chain hack. For that we need a separate cyber security act which will brings all the rules together in one place. It should be clearly written in it what is the function of CERT-In, NCIIPC,14C and should have the same rules for all sectors. How to do an attack report, how should security be reduced, how to disclose vulnerability.

Second, the establishment of the National cyber security Authority (NCSA). Now the work is done in different departments. That's why a single body is needed which will coordinate everyone. Just as the US has the office of the national cyber director and the EU has ENISA. Similarly, there should be a NCSA in India. It will look after the cybersecurity strategy of the entire country.

The NCSA should be able to supervise national cyber drills and resilience exercises in addition to coordinating threat intelligence sharing between the public and commercial sectors and standardizing incident reporting criteria across CERT-In, the DoT, the DPDPA, and sectoral regulators.

Third, statutory protections for online civil freedoms need to be reinforced. According to section 69 and 69A of the IT act, the government can monitor phones and internet. The paper argues that this power should be subject to a proportionality test and permission from an independent court. It means that no one should be spied on without reason. The government has been given an exemption in the name of national security in the digital personal data protection act. The paper argues that this should not be allowed to end data rights in general. It should be included only in special and urgent cases. Looking at the experience of ban on encrypted messaging apps in Jammu and Kashmir, the paper is saying that the government should get limited access in emergencies for the common people, apps like WhatsApp and signal should have E2E encryption. There should be a balance between security and privacy.

Fourth, India needs to invest more in its own infrastructure, personnel, and technology for cyber security.

Investing money in research into applied cryptography and AI security so that we can create our own secure tools. The teaching of cyber security should be expanded in universities. More engineers and experts need to be produced. Indian cybersecurity companies need to be given opportunities in government public procurement and helped to export so that they can go global. Sensitive government data and data of critical sections like power, bank should not be stored in foreign cloud AWS, azure. For this, India should create its own national cloud infrastructure which will create digital sovereignty.

Fifth, the report proposes that the cornerstone of India's sovereignty policy should be a clear, principal structure with three categories of data. Strictly localized data that will not go outside India such as defence, power grid, bank, hospital data, personal data like Aadhar. Free flow data that will go easily all over the world such as E-commerce, ads. And Bilateral agreement data that can only share with trustworthy countries like US, UE Japan. Security, trade, and clarity are all intended to be balanced by this tripartite classification. In addition to lowering trade barriers and avoiding too restrictive regulations that can impede economic integration and innovation, it safeguards justifiable national security concerns.

Sixth, India ought to participate more actively in the administration of cybersecurity worldwide. Discuss bilateral cyber talks with partners from important countries like US, EU, Japan. India should be active in multilateral forum like the UN group of governmental Experts (GGE) and the UN open-Ended working group (OEWG). Now the rules of the internet are mostly made by US and Europe. India can keep thew words of countries like the global south, Asia, Africa, Latin, America etc. There. India has got tier 1 status in ITU GCI 2024.so it is India's duty and obligation to take part in making international cyber rules.

7. Conclusion:

India's cyber security problem is not a tech problem. It is a governance problem. To prevent ransomware, hacking, espionage, simply buying a firewall or software is not enough. The real hard work is in creating these four things. they are institutional coherence means all departments work together without confusion, legal clarity means a clean and new cyber security law should be made, Democratic accountability means courts and people should check surveillance and power, and strategic capacity means that the country should have its own talent, tech, cloud. so that we do not have to depend on anyone else. If these four things are done, then we will not only save national security but also preserves the values of constitution, privacy and freedom.

The adoption of a data privacy law, the creation of national frameworks to safeguard critical infrastructure, international recognition for its cybersecurity posture, and the development of globally recognized digital public infrastructure are just a few of the noteworthy achievements India has made. In the areas of legislation, institutional coordination, human rights safeguards, indigenous talent, and strategic autonomy, there are still a lot of holes that need to be filled.

The stakes are really high. A major cyberattack on India's financial system, healthcare facilities, or electrical grid could have disastrous effects on the populace and the nation's economy. If encryption and privacy rights are violated in the name of security, the world's largest democracy may lose its democratic basis. Furthermore, an excessive dependence on foreign digital infrastructure could endanger India's geopolitical independence and provide foreign spies access to its most sensitive data. Overcoming these challenges requires political will, democratic discourse, and a 21st-century political structure in addition to technological know-how. Future studies should compare India's cybersecurity governance trajectory with that of similar middle-power digital economies in the Global South, evaluate the efficacy of CERT-In's enlarged audit system, and investigate the actual implementation of the DPDPA laws. Building an

evidence basis that could guide more effective policy will require both long-term analysis of cyber event data and qualitative evaluations of regulatory enforcement.

References:

1. Buzan, B., Wæver, O., & De Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.
2. Carnegie Endowment for International Peace. (2025, December 4). Mapping India's cybersecurity administration in 2025. https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025
3. Cavelty, M. D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and Engineering Ethics, 20(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y
4. Centre for International Governance Innovation (CIGI). (2024, December 4). India can be a pivotal player in stronger cybersecurity. https://www.cigionline.org/articles/india-can-be-a-pivotal-player-in-stonger-cybersecurity/
5. Chambers and Partners. (2025). Cybersecurity 2025 – India global practice guide. https://practiceguides.chambers.com/practice-guides/cybersecurity-2025/india
6. Deibert, R. J. (2013). Black code: Inside the battle for cyberspace. Signal.
7. 6clicks. (2025, September 1). India's critical infrastructure under siege: New CERT-In rules. https://www.6clicks.com/resources/blog/india-critical-infrastructure-cybersecurity-cert-in-audit-rules
8. Global Data Alliance. (2025). India's digital trade barriers. https://globaldataalliance.org/wp-content/uploads/2025/07/07022025gdaidusgdigitrade.pdf
9. Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. International Studies Quarterly, 53(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x
10. Internet Governance Project. (2024, October 21). Encryption under siege in India: National security and the erosion of digital privacy. https://www.internetgovernance.org/2024/10/20/encryption-under-siege-in-india-national-security-the-erosion-of-digital-privacy/
11. Jiang, M., Doshi, R., & Delgado, A. (2024). Models of state digital sovereignty from the Global South: Diverging experiences from China, India and South Africa. Policy & Internet, 16(4). https://doi.org/10.1002/poi3.427
12. Ministry of Electronics and Information Technology (MeitY). (2023). The Digital Personal Data Protection Act, 2023. Government of India. https://www.meity.gov.in
13. NASSCOM. (2025, December 16). India's steps towards a coordinated approach to cybersecurity. https://community.nasscom.in/communities/public-policy/indias-steps-towards-coordinated-approach-cybersecurity
14. NextIAS. (2025, August 2). India's digital sovereignty: Editorial analysis. https://www.nextias.com/ca/editorial-analysis/02-08-2025/india-digital-sovereignty
15. Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266
16. Padhai.ai. (2026, January 22). Cybersecurity: Definition, types and India's measures. https://padhai.ai/blogs-padhai/cybersecurity-in-india
17. Press Information Bureau (PIB). (2024a). Government of India taking measures to protect critical infrastructure and private data against cyber attacks.

https://www.pib.gov.in/PressReleasePage.aspx?PRID=2116341
18. Press Information Bureau (PIB). (2024b). Safeguarding India's digital landscape. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2037115
19. Recorded Future. (2021). China-linked group RedEcho targets the Indian power sector amid heightened border tensions. Recorded Future Threat Intelligence. https://www.recordedfuture.com
20. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382
21. Rau's IAS. (2025, December 1). Digital sovereignty: India's strategic imperative in the emerging tech order. https://compass.rauias.com/current-affairs/digital-sovereignty-india-strategic-imperative-emerging-tech-order
22. TechPolicy.Press. (2025a). India's search for digital sovereignty. https://www.techpolicy.press/indias-search-for-digital-sovereignty/
23. TechPolicy.Press. (2025b, January 23). Data localization: India's tryst with data sovereignty. https://www.techpolicy.press/data-localization-indias-tryst-with-data-sovereignty/
24. UpGuard. (2025, December 29). Top cybersecurity regulations in India in 2026. https://www.upguard.com/blog/cybersecurity-regulations-india
25. WebAsha Technologies. (2025, May 14). When did cybersecurity start in India? A timeline of events, laws, and milestones. https://www.webasha.com/blog/when-did-cyber-security-start-in-india-a-timeline-of-events-laws-and-milestones