International Journal of Sociology and Political Science
www.sociologyjournal.in
Online ISSN: 2664-7745, Print ISSN: 2664-7737
Received: 16-10-2025, Accepted: 15-11-2025, Published: 29-11-2025
Volume 7, Issue 4, 2025, Page No. 85-90

Surveillance, sovereignty, and strategic autonomy: India in the Indo-Pacific cyber order

Shreya Kasana
Research Scholar, Jawaharlal Nehru University Korean Studies, New Delhi, India

Abstract
Indo-Pacific is turning out to be the main rival in the global digital contest, where cyber power, information control, and technological reliance determine the strategic results. This environment poses some serious weaknesses as well as opportunities for India. This paper looks at the impact of surveillance politics, digital sovereignty needs, and strategic autonomy search on the changing cyber posture of India. It examines the threats of external intrusions of cyber-attacks, reliance on external technologies, and the role of domestic surveillance systems that are growing increasingly. At the same time, it assesses the diplomatic and institutional policies of India, including the law of data protection and local technological projects and cybersecurity efforts in collaboration with various options, including the Quad and the Indo-Pacific Oceans Initiative. The research paper holds on to the thesis that the capacity of India to be both open and closed, as well as be partnered and autonomous, will define its future cyber resiliency. Finally, the Indian model suggests a distinct example of going through the great-power rivalry without jeopardising the democratic digital governance.

Keywords: Surveillance politics, digital sovereignty, strategic autonomy

Introduction

The Indo-Pacific is rapidly turning into the centre of world geopolitical rivalry, and cyberspace is one of the most debatable and strategically important spheres (Shahin, 2024) [1]. With growing digital connectivity across the rest of the region, connecting the critical infrastructure, financial systems, defence networks, and civilian living, the Indo-Pacific cyber order is more influential in the trends of power, influence, and security. Key players like the United States, China, Japan and Australia are busy spending a lot of money on cyber capabilities, digital infrastructure and governing systems, making cyberspace one of the primary fields of technological contention, spying activities, and normative contestation (Bhattacharya, 2022) [2]. It is against this landscape that the idea of data sovereignty, secure supply chains, and dependence on technology have become the core of regional geopolitics (Chaisse *et al*., 2025) [3]. To India, whose society is quickly being digitalised and its position as a power on the rise in the Indo-Pacific, there are both critical weaknesses and operational prospects presented by this changing environment. The increasingly digital environment of India, which is typified by mass public digital infrastructure, the rise of cyber threats, and increasing economic-technological interdependence, needs a consistent cybersecurity environment that meets the national interests and does not jeopardise economic growth (Nachiappan, 2022) [4]. India's foreign policy tradition of strategic autonomy only exacerbates India's cyber decisions, especially in an environment that is becoming competitive in the US-China technological rivalry. The need to maintain independence in making digital policy choices and cooperation with like-minded partners is consequently a major challenge.

The research will attempt to explain how India makes its cyberspace policy in such dynamic relationships, and how its quest to achieve strategic autonomy affects the decisions made in this sphere on issues concerning data governance, cybersecurity collaboration, and technological associates. It assesses the policy trends, institutional processes and diplomatic efforts of India and how these have affected the national security and the stability of the region. The purpose of this research is to place India in the context of cyber posture within the Indo-Pacific, to point out the issues, the contradictions, and the opportunities that direct how India is trying to navigate a changing digital landscape at high velocity. Finally, it is relevant to scholarly and policy discourses regarding cyber governance, strategic autonomy and the future of the Indo-Pacific security architecture.

Research Objectives

1. To examine the evolving Indo-Pacific cyber landscape and identify the key geopolitical, technological, and governance trends shaping regional cybersecurity dynamics.
2. To analyse India's cyber vulnerabilities and strategic priorities, focusing on how surveillance threats, data governance challenges, and technological dependence influence national security considerations.
3. To evaluate India's pursuit of digital sovereignty and strategic autonomy in the context of intensifying US-China technological rivalry and shifting regional cyber alliances.
4. To assess the effectiveness of India's institutional, legal, and diplomatic frameworks, including cybersecurity agencies, data protection laws, and Indo-Pacific partnerships in enhancing cyber resilience.
5. To explore India's role in shaping the Indo-Pacific cyber order, particularly through initiatives such as the Quad, digital public infrastructure diplomacy, and multilateral cyber governance efforts.

Theoretical Basis of India's Cyber Strategy

The multi-layered theoretical framework that brings together cyber power, digital sovereignty, surveillance models, and international relations perspectives is needed in comprehending the role and status of India regarding the

emergent Indo-Pacific cyber order (Ain & Bukhari, 2024). Simply put, cyber power refers to the ability of a state to apply digital instruments in the defence, influence and coercion. It has typologies such as cyber capability (technical and institutional strength), cyber dependence (reliance on foreign hardware, software or infrastructure) and cyber coercion (that is, use of cyber operations to intimidate or influence state behaviour). Those types assist in evaluating the current cyber preparedness of India and the boundaries created due to technological dependency on foreign actors (Garge, 2025) [6]. The framework is also based on the theories of surveillance capitalism and state surveillance models, which distinguish between the US model of data capture in the private sector, the Chinese model of state-controlled digital ecosystems, and mixed forms of surveillance used in various democracies. The comparison of these systems is important in situating the situation of digital regulation, data sovereignty, and cybersecurity governance in India, particularly as the country is starting to decide on balancing the needs of economic openness and national security interests (Fernandes & Abosata, 2024) [7]. The third conceptual pillar is strategic autonomy, an ancient tenet in Indian foreign policy which has been transferred to the digital world. In the case of cyberspace, strategic autonomy can be defined as India being an independent decision-maker, not overdependent on any other significant power, and not needing to create its own technological environment. There are other insights in international relations theories. From a realist view, cyberspace is a war zone and a contested plane and a security dilemma field, which is orchestrated by the rivalry of the major powers. A liberal institutionalist approach focuses on the cooperative norms, multi-stakeholder governance, and international cyber frameworks. In the meantime, a constructivist lens emphasises the influence of identities, values, and digital norms on India's decision-making on aspects like data protection and democratic governance (Baldoni & Di Luna, 2025) [8]. Combined, these constructs offer a comprehensive contextual basis for the analysis of the cybersecurity strategy of India alongside its pursuit of resilience and independent control in the Indo-Pacific.

The Indo-Pacific Cyber Landscape

The complex interaction between technological rivalry, modes of governance, and changing security threats defines the cyber environment in Indo-Pacific as an indicator of the geopolitical transformation in the area (Ain & Bukhari, 2024) [5]. Large participants are vigorously employing cyber capabilities to broaden control and acquire online space. At its core is the Digital Silk Road of China, which is comprised of both large-scale digital infrastructure, export of surveillance technologies and more sophisticated offensive cyber capabilities, which not only expand its geopolitical capacity but also its intelligence operations (Garge, 2025) [6]. The United States reacts to this through marketing an open, interoperable, and secure internet by outsourcing its supremacy in cloud services, online platforms, and alliances with its allies in setting standards globally. In the meantime, such middle powers as Japan, South Korea, and Australia, and ASEAN states are increasing national cyber infrastructures and taking part in inter-regional efforts to become more resilient to the external network and decrease reliance on it (Fernandes & Abosata, 2024) [7]. In this climate, there have been long-standing conflicts regarding the control of data over cyber-governance, particularly between the policies of localisation of data that are implemented by various states and the model of cross-border data flow that is preferred by the world's technological giants (Baldoni & Di Luna, 2025) [8]. The regional order is also compounded by national firewalls, content regulation regimes, and dependency on foreign hardware and software. The security issues are also increasing because cyber spy attacks and ransomware attacks, digital piracy, and hybrid warfare are occurring more and more often, and in more advanced forms. The critical infrastructure, including power grids, shipping ports, energy systems, and telecom networks, is more exposed to state-sponsored attacks and criminal networks, which makes the vulnerability of supply chains and systemic failure a cause of concern. Moreover, the marine environment is becoming a hub of cyber threats, whereby naval infrastructure, offshore energy assets, and commercial shipping routes, which are important to trade in Indo-Pacific, are affected. Collectively, these forces highlight the stakeholder-based nature of the regional environment where regional states need to develop cyber strategies that associate openness, security, sovereignty, and technology independence.

Surveillance, Politics and Cybersecurity Threats for India

Internal Surveillance Dynamics

There has been a proliferation of the internal surveillance environment in India in the last ten years as the Indian state attempts to reinforce national security, hinder terrorism and regulate massive-scale digital government (Azevedo *et al*., 2025) [9]. The increasing institutionalisation of surveillance capabilities is reflected in systems like NATGRID that gather the data collected by different agencies, as well as systems like the Central Monitoring System (CMS) that allow real-time interception of communications. Automated Facial Recognition System (AFRS) and other biometric programs also make the state increasingly aware of citizen behaviour, and digital health apps such as Aarogya Setu, in response to the COVID-19 pandemic, created a nationwide debate about the privacy and transparency of data. Even though these tools have significant security purposes, they also create massive concerns regarding management, proportion, and misuse of these tools. The lack of strong judicial/parliamentary checks increases concerns about the loss of privacy and algorithmic profiling (Shah & Dar, 2025) [10]. India is grappling with the dilemma between the need to achieve national security and the establishment of a networked design of governance, and the constitutional clause of freedom and the right to liberty. The strain influences the wider discussions about the sovereignty of states online and the moral limits of state power within cyberspace.

External Cyber Threat Landscape

Most external threats are evidenced by an intricate and growing hostile cyber threat landscape outside India, marked by state-backed hacks, campaigns of hybrid warfare, as well as advanced criminal beta networks. China has still been the largest cyber threat, and it has been reported numerous times that they have targeted and intruded on the Indian power grids, telecom infrastructure, and railways,

among other sensitive areas (Patil, 2025) [11]. The objectives of these cyber activities, in most cases, include gleaning intelligence, interrupting service or leaving latent vulnerabilities in critical infrastructure. Pakistan, in its turn, conducts a set of hybrid propaganda operations, cyber-misinformation, and other low instrumental cyber operations that would destabilise the social harmony and enhance political polarisation in India. In addition to the role of state actors, India experiences an increase in cybercrime due to the global ransomware groups, financial fraud syndicates, and phishing networks, which seize the loopholes in digital literacy and preparedness in institutions. All these actions serve to diminish the economic security and the trust of citizens in the virtual structures. The external cyber threat environment is also complicated by further growth of cyber tools, dark-web markets and the growing application of artificial intelligence to malicious intent (Sharma, 2025) [12]. To India, such issues highlight the importance of powerful defensive support, better intelligence coordination, and a robust alliance with like-minded states in the Indo-Pacific.

India's Vulnerabilities

Within the current developments in the world of cybersecurity policy and institutional maturity, India is still struggling with the overwhelming structural and strategic weaknesses (Azevedo *et al*., 2025) [9]. One of the weaknesses is that it largely relies on foreign hardware, such as Chinese-made network equipment, which exposes the supply chain risk is serious; it exposes the supply chain to significant backdoor risks. The fact that the country is experiencing semiconductor shortages also further hinders its capabilities of achieving technological independence. Moreover, being underinvested in offensive cyber capabilities, India influences the deterrence posture since a functional cyber strategy frequently involves the ability not only to counterattack but to demonstrate the power of retaliation. The other major problem is the complexity of the laws and regulations that regulate cyberspace. The impossibility of harmonious national governance is caused by overlapping mandates among the agencies, old cyber legislation, and standards of data protection that are not uniform (Shah & Dar, 2025) [10]. Lack of a centralised cybersecurity legislation leads to a lack of clarity in accountability, reporting of cyber-incidents, as well as in the coordination of institutions. Furthermore, weak cyber hygiene among the departments within the governments and operators of critical infrastructure contributes to vulnerabilities (Patil, 2025) [11]. Such issues of structure, along with the fast growth of digital space and the growing dependence on cloud solutions and interdependent systems, contribute to India becoming a favourable target of opponents (Sharma, 2025) [12]. These gaps need to be remedied to enhance the cyber resiliency of India and to allow the latter to have a real strategic independence in the Indo-Pacific digital order.

India's Digital Sovereignty Strategy

Data Governance and Legal Architecture

The strategy of digital sovereignty in India is rooted in a transforming legal and regulatory framework that would enhance the protection of data, hold the accountable and help in securing the digital ecosystem (Lissy, 2025) [13]. Efforts to enhance privacy. The Digital Personal Data Protection (DPDP) Act 2023 is also a landmark with its provisions creating a guideline concerning the lawful use of personal data, consent of a user, and access to personal data by a state. As the Act increases user rights, it has wide exemptions to government agencies, which, to some other critics, raise concerns about oversight and privacy security (Chaudhary, 2023) [14]. This is augmented by the suggested Digital India Act, which is to help modernise the cyber law in the country by supplanting the old IT Act 2000. It will focus on dealing with new issues that include misinformation, deepfakes, cybersecurity principles, and how digital platforms should be governed. There is also the enforcement of data localisation requirements in India, where sensitive data needs to be stored or processed in the domestic territory to limit exposure to foreign surveillance and enhance regulatory control. CERT-In guidelines on the timing of breach reporting and log retention are also supplementary measures to cyber accountability. Combined, these structures are an indication of India being passionate and determined to make digital governance consistent with national security issues, even as it tries to develop a rights-based, open system that fits well in a fast-growing digital economy.

Technological Self-Reliance (Atmanirbhar Cyber Ecosystem)

The technological self-reliance is a fundamental aspect of the Indian digital sovereignty strategy, which is projected as part of a larger vision of Atmanirbhar Bharat (Kailas Nath, 2025) [15]. India has realised that overreliance on foreign technologies can be quite a risk; this has seen the country increase its efforts in developing local digital infrastructure and high-tech solutions. At the core of this can be seen the push of domestic 5G and new 6G innovation, enabling co-operation between research institutions, individual telecoms and government agencies. Meanwhile, the mission of India Semiconductor seeks to have a strong chip manufacturing ecosystem to alleviate the vulnerability of supplies in the global supply chain and decrease dependency on foreign vendors. Sovereignty in the clouds is also on the agenda, and there are efforts to promote cloud platforms run by Indians as well as data centre localisation. These activities are accompanied by investments into native cybersecurity tools, encryption technology, and AI-based threat detection systems. Although development is still uneven as far as the technological disparity and the capital intensity are concerned, the trend of becoming independent also gives signals to the long-term perspective of building the strengths of strategic independence in India. India aims to make its digital infrastructure more geopolitically resistant, secure, and less vulnerable by creating homegrown solutions to important industries like telecom gear and other internet of things devices, operating systems, and more.

National Cyber Institutions

The institutional strengthening is a very significant element of the digital sovereignty agenda in India (Vinodan & Kurian, 2024) [16]. The nation has developed a multilayered system of national cyber institutions to synchronise security, incident response and policy implementation. CERT-In is the agency of reference in responding to cybersecurity incidents, providing guidelines, organising and ensuring continuity of digital services. The National Critical Information Infrastructure Protection Centre (NCIIPC) has a limited role of protecting critical areas like energy, finance,

transport, and defence. A supplement to these civilian organs, the Defence Cyber Agency (DCA) strengthens military preparedness through the combination of offensive and defensive cyber operations. Digital governance reform is made through the Ministry of Electronics and Information Technology (MeitY), and telecom cyber hygiene, equipment screening, and spectrum governance go through the Department of Telecommunications (DoT). The National Security Council Secretariat (NSCS) performs strategic leadership by facilitating inter-agency coordination and the development of national cyber doctrines. Cyber cells and forensic laboratories have also grown in states, and threat intelligence sharing, together with capacity building of both the state and public-private collaboration, are enhanced through the use of public-private partnerships. Although there has been improvement, coordination, resource and jurisdiction remain a challenging issue. Nevertheless, this institutional network can be viewed as the core of the Indian practices in ensuring its digital environment and gaining control in an intricate cyberspace.

Balancing Openness and Control

The digital sovereignty strategy has to be characterised by a fine balance between openness and commitment to global innovation, and regulatory control as a measure to protect national interests, which has to be taken in India (Ranjan, 2025) [17]. To prevent the profound reliance on either Western technology giants or Chinese digital infrastructures, the government, in particular, is concerned with the geopolitical competition. This balancing is experienced in the selective ban on Chinese telecommunications equipment vendors, cautious participation in cloud and platform providers of the U.S., and support of domestic substitutes. The suggested digital competition legislation to be used should serve to enhance the regulation of dominant architectures, promote healthy competitiveness and curb the threat of monopolistic domination of Indian data and digital markets (Bhattacharya, 2022) [2]. At the same time, to keep the economic growth and technological improvement, India is still a proponent of open standards and international interoperability. The difficulty is in combining local innovation by not shutting off Indian markets or silencing international digital channels. The strategy India follows combines regulatory boldness, through localisation requirements, platform regulation standards and content moderation models, with liberalism towards international cooperation, particularly in such initiatives as the Quad, EU-India digital partnerships and global digital public infrastructure diplomacy (Nachiappan, 2022) [4]. This two-step approach depicts an Indian attempt to establish a digital route where India will maintain levels of independence, yet still be a part of the global digital networks, which will secure and innovate India in the future.

India's Strategic Autonomy in the Indo-Pacific Cyber Order

The necessity to balance the growing US-China technological competition is what determines the development of strategic autonomy in the Indo-Pacific cyber order and the growth of the independent digital agenda of an independent digital vision based on security, sovereignty, and innovation in India (Garge, 2025) [6]. India has gone on record to restrict access to Chinese telecom giants of Huawei and ZTE on grounds of espionage, vulnerabilities in their supply chains, and security of the critical infrastructure. Such limitations bring India closer to the wishes of its partners in the West, although New Delhi is not fond of relying on a particular bloc. It has increased its cyber cooperation with the United States, Japan, Australia and the European Union, including the exchange of information, cyber hygiene provisions, cooperative use of technology, and capacity building (Baldoni & Di Luna, 2025) [8]. In the Quad, India fully partners on the formulation of a democratic cyber agenda of resilient supply chains, secure critical technologies, and countering digital authoritarianism that generates convergence and autonomy in its strategic positioning. In addition to great-power politics, the Indo-Pacific policy of India supports its autonomous policy. The Indo-Pacific Oceans Initiative (IPOI) incorporates cyber-marine resiliency, which deals with the vulnerability in maritime communications, port logistics, and undersea cable networks. Other areas where India conforms selectively with the ASEAN Digital Masterplan include focusing on regional interoperability and inclusive digital development, providing cyber training and digital infrastructure assistance to littoral states in the Indian Ocean. Such alliances empower India without making it commit to a strict form of alliances. Global export of Digital Public Infrastructure (DPI), which comprises systems like UPI, Aadhaar-enabled, and India Stack, is a significant foundation of India's autonomous digital strategy. India is becoming a digital powerhouse by encouraging secure, affordable, interoperable digital solutions that provide an alternative to the Silicon Valley systems and the state-focused networked digital models of China. Cumulatively, these efforts are used to explain how India is an Indian country using cyber diplomacy, technological innovation, and selective alignment to exude strategic autonomy in an Indo-Pacific cyber competitive environment.

Challenges to India's Cyber Strategy

The cyber strategy in India is confronted with an intricate structure, external, and normative set of obstacles that cumulatively prevent the formation of a robust and independent digital security infrastructure (Shah & Dar, 2025) [10]. Strategically, the ecosystem is plagued by an acute talent crunch, bureaucratic overlaps, and a disjointed regulatory environment that slows down decision-making and institutional coordination. The lack of rigorous local development and research into cybersecurity further increases reliance on imported technologies at key levels of the digital stack, such as cloud platforms, chipsets, operating systems, and sophisticated cyber defence applications, which in turn are controlled by US-aligned companies (Sharma, 2025) [12]. On the external front, India may have to grapple with a more aggressive behaviour of cyberspace, which possibly has been created by the Chinese, by its aggressive and unfriendly cyber activities, spy attacks, and rapid South-Asian digital growth by telecoms infrastructure, cyber surveillance systems and cyber public goods. Such aspects have global weaknesses in terms of strategies and limit the technological creativity of India. Coupled with the above material constraints, the cyber strategy should address highly political and ethical challenges in India. Constant preoccupation with the issues of privacy breach, the boundaries of democratic accountability, and the secrecy of surveillance operations does not contribute to governmental credibility among the population. The tedious task of

balancing the harmful online content with ensuring the freedoms of expression still poses a thorn in the flesh, especially in an electoral democratic system where the digital platforms become the instruments of shaping politics. The content moderation regimes are subject to either overreach or ineffectiveness, which has high democratic costs. In the meantime, the possibility demonstrated with the growth of state and non-state surveillance opportunities, which may manifest as facial recognition, data control, or predictive policing, provokes concern about the intrusion of the state and a decrease in civil rights. Combined, these structural, geopolitical and normative pressures suggest that the cyber strategy in India needs to be developed not only by developing technological capability but also by redesigning its institutions, ethical protection and better articulation of democratic Internet governance.

Policy Recommendations

A package of coordinated policy interventions to strengthen the capabilities of India, modernise regulation, increase technological self-reliance, and increase diplomatic efforts can enhance the cyber strategy of India (Lissy, 2025) [13]. On the operational level, an integrated cyber command would be assigned with a clear mandate on defence, deterrence and proportional offensive action, which would raise the capability of India in responding to advanced attacks (Chaudhary, 2023) [14]. Periodic red-teaming in the government as well as in the critical sectors, along with enhanced cyber hygiene standards, would mitigate the exposure of the critical infrastructure facilities like energy, finance, transport, and digital public facilities (Kailas Nath, 2025) [15]. Legally and at the state regulatory level, India badly needs to have balanced cybersecurity laws that specifically define cybercrimes, set standard laws and implement control measures to prevent the high extent of surveillance and accountability. Increasing judicial and legislative questions of interception and surveillance systems would also increase trust (Vinodan & Kurian, 2024) [16]. The creation of technological self-reliance is a paramount strategic challenge; this involves hastened creation of a domestic semiconductor environment, specific funding on local encryption systems and the establishment of secure and diversified supply-chain networks with dependable partners to ease reliance on foreign hardware and software (Lissy, 2025) [13]. Similar initiatives should be used to facilitate the development of Indian cybersecurity start-ups by reforming procurements and conducting research (Chaudhary, 2023) [14]. India should be more proactive in advancing international cyber norms, especially in data sovereignty, responsible state action and the digital frontiers of cross-border flow, and engage in more bilateral and multilateral cyber discussions with key partners in a diplomatic fashion (Kailas Nath, 2025) [15]. It is also possible to enhance the influence of India in the whole of the Global South by endorsing the Digital Public Infrastructure (DPI) model of India as an alternative to the Chinese digital ecosystem, which is constructed on the principles of openness, inclusion, and interoperability (Vinodan & Kurian, 2024) [16]. The combined effect of these policy measures would not only strengthen India against the rising cyber-attacks but also force the country to become a normative and technological flag bearer in the new global cyber balance.

Conclusion

The changing role of India in determining the Indo-Pacific cyber order is based on a multifaceted game of surveillance requirements, digital sovereignty, and the desire to achieve strategic independence, which will shape the outlines of its technological future. With the region turning into a battleground of the US and China's technological confrontation, India has to juggle between opposing demands and implement a cyber strategy to ensure national security without losing its democratic spirit. Such a dualism of the challenge to gain cyberspace and retain an open, rights-based digital identity requires a fine-tuned strategy of enhancing the capacity of states, but does not allow the tendency toward uncontrolled surveillance and over-centralisation. The focus on making India technologically autonomous, in terms of indigenous infrastructure, encryption, semiconductors, and cyber technologies, should be served by initiating responsible international cooperation by the Quad, the ASEAN models, as well as collaborating with reliable digital democracies. Simultaneously, the growing number of diplomatic activities of India, in particular via Digital Public Infrastructure (DPI) exports, makes it a normative influence on a uniform and interoperable digital ecosystem of the Global South. Future studies need to explore further into the cyber deterrence posture of India, AI systems governance, and maritime cyber vulnerability throughout the Indo-Pacific region, as well as make comparisons on digital governance within the area. An entire academic involvement in these new themes would not merely shed light on strategic directions of India, but would also emphasise how the nation could, at the same time, claim an independent view, be security conscious, and nurture the democratic principles underpinning the digital ascendancy of the country.

Reference

1. Shahin J. Dancing to the same tune? EU and US approaches to standards setting in the global digital sector. Journal of European Integration,2024:46(7):1111–1131. https://doi.org/10.1080/07036337.2024.2398430
2. Bhattacharya D. India’s cyber security policy: Strategic convergence and divergence with Quad. Institute for Security and Development Policy, 2022. https://www.isdp.eu/publication/indias-cyber-security-policy
3. Chaisse J, Dimitropoulos G, Valderrama IJM. Advancing digital integration in the Indo-Pacific – Legal strategies for a cohesive digital economy. In A. Prakash (Ed.), Global value chains of digital economy in the Indo-Pacific: Challenges and opportunities. ERIA, 2025, 1–20. https://www.eria.org/uploads/1_ch_1-Advancing-Digital-Integration-Legal-Strategies.pdf
4. Nachiappan K. Going on the offensive: India’s cyber capabilities. NUS Institute of South Asian Studies, 2022. https://www.isas.nus.edu.sg/papers/going-on-the-offensive-indias-cyber-capabilities
5. Ain QU, Bukhari SS. The grand Indo-Pacific chessboard: India’s role its geostrategic imperatives. Indian Journal of Asian Affairs,2024:37(1–2):73–84. https://www.jstor.org/stable/27359396
6. Garge R. India as the anchor (stabilizing force) of the Indo-Pacific in the era of the roaring 40s. Security

Science Journal, 2025. https://www.securityscience.edu.rs/index.php/journal-security-science/article/view/170
7. Fernandes Y, Abosata N. Analysing India's cyber warfare readiness and developing a defence strategy. arXiv, 2024. https://arxiv.org/abs/2406.12568
8. Baldoni R, Di Luna G. Sovereignty in the digital era: The quest for continuous access to dependable technological capabilities. IEEE Security Privacy,2025:23(1):91–96. https://doi.org/10.1109/msec.2024.3500192
9. Azevedo AC, Scheid EJ, Franco MF, Granville LZ. Assessing SSL/TLS certificate centralization: Implications for digital sovereignty. arXiv, 2025. https://arxiv.org/abs/2504.16897
10. Shah PIA, Dar ZA. India's strategic engagement in the Indo-Pacific: A blueprint for regional security. South India Journal of Social Sciences,2025:23(5):62–65. https://doi.org/10.62656/sijss.v23i5.2103
11. Patil S. The digital Silk Road and smart city networks in the Indo-Pacific: A primer. ORF, 2025. https://www.orfonline.org/research/the-digital-silk-road-and-smart-city-networks-in-the-indo-pacific-a-primer
12. Sharma S. How emerging tech is reshaping Indo-Pacific security. ORF, 2025. https://www.orfonline.org/expert-speak/how-emerging-tech-is-reshaping-indo-pacific-security
13. Lissy T. Bridging digital divides: India's cybersecurity gaps and the case for US–India cooperation. Geopolitical Monitor, 2025. https://www.geopoliticalmonitor.com/bridging-digital-divides-indias-cybersecurity-gaps-and-the-case-for-us-india-cooperation
14. Chaudhary PK. India's cybersecurity diplomacy: Building global alliances. ShodhKosh Journal of Visual and Performing Arts, 2023, 4(2). https://doi.org/10.29121/shodhkosh.v4.i2.2023.3386
15. Kailas Nath G. Autonomy and cooperation: India's engagement in the Indo-Pacific. International Journal of Social Science and Human Research, 2025, 8(5). https://doi.org/10.47191/ijsshr/v8-i5-25
16. Vinodan C, Kurian AL. Strategic autonomy and India's hedging policies in the Indo-Pacific. Journal of Asian Security and International Affairs,2024:11(4):475–495. https://doi.org/10.1177/23477970241282095
17. Ranjan NDVU, DK. India's Indo-Pacific strategy: A masterclass in strategic balancing. Knowledgeable Research: A Multidisciplinary Journal,2025:4(2):86–89. https://doi.org/10.57067/a3cwd594