# CYBERDIPLOMACY AND THE NEW DIGITAL NON-ALIGNMENT IN THE GLOBAL SOUTH: INDIA AS A CASE STUDY OF TECHNOLOGICAL SOVEREIGNTY IN THE AGE OF AI

**Daria-Elena POPESCU**
Master's Student in Security and Technology, Department of International Relations and European Integration, National University of Political Studies and Public Administration,
daria.popescu.22@student.politice.ro

**Abstract:** In the context of growing fragmentation in the global cyber order and intensifying competition over international digital norms, nations in the Global South seek autonomy in a landscape dominated by major technological powers. Among these actors, India stands out for its hybrid diplomatic strategy, carefully avoiding full alignment with either Western liberal frameworks or authoritarian digital governance models. This article explores India's digital diplomacy as an emblematic case of "digital neo-nonalignment"—a strategic posture aimed at safeguarding infrastructural sovereignty, regulatory autonomy, and normative influence in the global AI governance. Through analysis of strategic initiatives such as Digital India, IndiaAI, and the Data Empowerment and Protection Architecture (DEPA), the study examines India's distinctive path, highlighting implications for the emerging normative architecture of the AI and digital governance globally.
**Keywords:** Cyberdiplomacy, digital non-alignment, digital sovereignty, India, Global South, AI governance, DEPA, Digital India, global norms, strategic autonomy.

## INTRODUCTION

The global digital order is at a crossroads, characterized by a pronounced polarization into competing normative frameworks. On one hand there lies the Western liberal approach, emphasizing openness, transparency, and privacy rights; on the other, the authoritarian digital governance model, exemplified primarily by China, prioritizing centralized control, digital surveillance, and sovereign technological ecosystems. Yet, between these poles, an alternative strategic narrative is emerging—one that does not align comfortably with either paradigm. This phenomenon, best described as the "digital neo-nonalignment," is shaping the diplomatic and technological trajectories of the states within the Global South, offering a compelling alternative to the prevailing models of the digital sovereignty.

In this emerging context, India becomes a particularly salient case study—both for its historical non-aligned legacy and its current technological ascent. Within this shifting landscape, India emerges as a critical case study, leveraging its substantial technological sector and strategic positioning to assert a nuanced form of autonomy. India stands at the forefront of this evolving strategic landscape, uniquely positioned as both an emergent technological power and a pivotal diplomatic actor. Characterized by its robust IT sector, rapid digitalization, and substantial demographic dividend, India consciously avoids a full integration into either of the dominant global digital frameworks. Instead, it engages in a strategic form of digital diplomacy that

can be aptly described as a "neo-digital non-alignment," carefully balancing sovereignty, technological autonomy, and international cooperation.

Historically, India's diplomatic identity has roots in the Non-Aligned Movement (NAM), articulated during the Bandung Conference of 1955, which sought to carve a path independent from the Cold War blocs. Today, facing a new "digital Cold War," India employs an analogous yet distinctively modernized diplomatic logic. Through deliberate and sophisticated hedging strategies, the country avoids any overt commitment to either digital superpower, while simultaneously engaging extensively with global normative debates, technological standard-setting forums, and regulatory initiatives.

The rapid diffusion of digital technologies has transformed the cyberspace into a critical frontier of international relations, particularly for the emerging economies seeking to leverage digital tools for their development and global influence. The accelerating pace of digital transformation has elevated cyber diplomacy into a central axis of global governance and strategic competition. For the emerging powers in the Global South, most notably for India, the dual imperative of harnessing digital opportunities and safeguarding strategic autonomy is reshaping their international engagement —creating a distinctive form of non-aligned cyber statecraft in the process. Against this backdrop, this article examines how India is forging a hybrid diplomatic posture—anchored in claims of digital sovereignty, multi alignment, and norm entrepreneurship in global forums.

India reflects these strategic priorities not only at the declarative level, but also through its internal architecture of digital public policies and diplomatic initiatives.

India’s increasing role in cyber diplomacy is both strategic and symbolic. Homegrown initiatives such as the IndiaAI Mission, which finances indigenous compute infrastructure and aims to cultivate sovereign large language models, reflect a broader vision: asserting normative autonomy while participating in multilateral regimes like the UN, G20, and concurrently, New Delhi’s drive to export Digital Public Infrastructure—rooted in the success of Aadhaar and UPI—signals a willingness to offer an alternative governance template for the digital age Financial Times (Bandura, McLean & Smutny, 2024; Smart Partnerships, 2021; Ministry of Electronics and IT, 2025).

However, India's positioning does not follow a rigid doctrine, but expresses a form of strategic maneuvering specific to emerging actors. Yet this strategic posture is not doctrinally tidy; India’s approach exemplifies what the scholars of the cyber statecraft term the "middle ground" — balancing ties with liberal democracies and authoritarian powers alike, while safeguarding flexibility and agency online. Such maneuvering echoes the historic Non-Aligned Movement, yet adapts it to the digital age: India opts neither for uncritical alignment nor for isolation, but for a third way of digital non alignment, bolstered by institutional autonomy and normative leadership potential.

This position has significant implications for the entire architecture of the global digital governance.

The stakes are consequential. As the digital technologies—particularly AI, quantum computing, and blockchain—reshape global power structures, India’s ability to influence rule setting for governance, interoperability, and cyber norms will affect the strategic options of many Southern actors. In the absence of robust domestic codification or doctrinal clarity, its

evolving posture nevertheless signals an emergent model: a digitally confident Global South actor bridging development objectives with normative agency in cyber diplomacy.

India's concerted push towards a digitally empowered society underscores the broader relevance of cyber diplomacy: it offers pathways to economic growth, governance innovation, and strategic autonomy to emerging economies in a contested digital order. According to the Data Security Council of India, India's core digital sectors accounted for approximately 7 percent of GDP in 2017–18 and are projected to grow to 8–10 percent by 2025, highlighting the strategic stakes of integrating cybersecurity into national policy (Data Security Council of India, 2020).

At the heart of India's digital acceleration is the Digital India programme, launched to bridge the gap between the "digital haves" and "have-nots" by deploying cloud computing, mobile applications, and high speed internet as core utilities. By 2019, nine pillars—ranging from cradle to grave digital identity to shareable private space on public cloud—were set to galvanize citizen empowerment and inclusive growth (Government of India, 2015). This digital transformation not only promises to enhance service delivery and financial inclusion but also to underpin India's comparative advantages in technology-driven governance and its strategic positioning in the global cyber forums.

The strategic stakes of cyber diplomacy for India—and by extension for other emerging economies—are fourfold:

1. Access to the digital technologies for economic growth, ensuring that firms and citizens alike can harness ICT infrastructure for productivity gains (Data Security Council of India, 2020) .
2. Representation in the global governance of emerging technologies such as AI, data flows, and cyber norms, where India champions a principle of "data sovereignty" to safeguard national interests (PwonlyIAS, 2024) .
3. Autonomy in the implementation of transformative technologies in the military domain, maintaining sovereign control over critical cyber capabilities amid great power competition.
4. Long term sustainability through national digital industries, from semiconductors to AI research platforms, fostering an indigenous technology ecosystem.

This article offers the first academic analysis of India's cyber diplomacy as a case study for the Global South agency in shaping global norms, demonstrating how New Delhi's normative agenda—anchored in digital sovereignty and non alignment—provides a model for other emerging economies. The article offers India as an empirically grounded case study of digital non-alignment and cyber diplomacy in the Global South. We trace New Delhi's participatory strategies in multilateral forums, its domestic policy architecture for sovereign AI and data, and its bilateral and regional practices—from "digital dosti" technology diplomacy to partnerships with the Quad and SCO.

Central to India's strategic calculus is the management of its technological sovereignty, particularly regarding artificial intelligence and data governance (Patel & Shrivastava, 2025; Digital India, 2023a, 2023d; PRS Legislative Research, 2023). The proliferation of AI technologies has raised profound concerns about sovereignty, security, and the ability of nations to independently regulate, innovate, and deploy transformative digital infrastructures

(Jensen & Atalan, 2025; UNIDIR, 2021; Innovation in Defence Services & Technology, 2022). India, equipped with a thriving IT sector, initially built upon outsourcing and offshoring—collectively symbolized by its renowned "WITCH" companies (Wipro, Infosys, Tata Consultancy Services, Cognizant, and HCL)—views its ability to shape its AI governance not only as a means of economic advancement but also as an instrument of geopolitical leverage and normative influence (Chair on India and Emerging Asia Economics, 2024; Tomoshige, 2023; Basu, 2022; Lewis, 2024; Bandura, McLean & Smutny, 2024).

Given these stakes, understanding India's hybrid cyber diplomatic approach becomes crucial. The article thus investigates several core dimensions:

- Strategic autonomy: How India's initiatives such as Digital India, DEPA, and IndiaAI illustrate a deliberate effort to maintain an infrastructural independence and a regulatory discretion.
- Normative impact: How India's distinct positioning may influence the emerging global standards, especially concerning AI ethics, data privacy, and cross-border digital governance.
- Global South leadership: Whether India's model can serve as a credible alternative for other emerging nations seeking a similar balance between openness and state sovereignty in the digital sphere.

This analysis is not merely descriptive; it also holds a prescriptive significance. By examining India's diplomatic and regulatory innovations, policymakers, scholars, and practitioners can glean the insights into effective digital governance strategies in a multipolar technological landscape. The stakes involve not only national sovereignty but the broader architecture of a global digital governance—an issue of critical significance as nations worldwide navigate the complexities of the AI era.

As such, the following article first contextualizes the polarization of the global digital order, then positions India within the emerging paradigm of the digital neo-nonalignment. Subsequently, it scrutinizes specific Indian strategic and legal initiatives and evaluates their implications for the global governance standards. Ultimately, the analysis underscores cyber diplomacy's transformative potential as a negotiation space for technological sovereignty in an age increasingly defined by artificial intelligence.

This analysis is guided by clear research questions, which reflect the strategic, normative, and doctrinal dimensions of the phenomenon:

1. What precisely constitutes a "digital nonalignment," and how does India operationalize this concept as a strategy of digital non alignment through cyber diplomacy and sovereign infrastructure?
2. What normative claims and institutional mechanisms support its role in the global governance of emerging technologies?
3. In what ways does India's posture compare with the classical non aligned political theory and prompt a new conceptual category—cyber non alignment?
4. What implications does India's distinctive diplomatic positioning have for the evolving global frameworks governing AI, cybersecurity, and data sovereignty?

5. Can India's approach serve as a viable alternative model for other nations of the Global South, navigating between polarized digital governance paradigms?

Following this introduction:

- Section 2 situates the concept within broader debates on digital sovereignty and normative contestation in the contemporary digital order.
- Section 3 presents India as a hybrid actor: domestically cultivating sovereign AI and public infrastructure, regionally exercising hedging strategies, and globally shaping norms through forums such as GPAI, G20, and UN cyber norm discussions.
- Section 4 frames the strategic and normative implications—for standard setting competition, technological autonomy in the Global South, and normative influence.
- The conclusion offers policy reflections on how cyber diplomacy may redefine sovereignty in the AI era and suggests generalizations for other developing states.

## POLARIZATION OF THE DIGITAL ORDER AND THE EMERGENCE OF THE GLOBAL SOUTH

In recent decades, digital technologies have profoundly reshaped the foundations of international relations, security, and governance, catalyzing a dramatic restructuring of the global geopolitical landscape. Amid these transformations, the governance of cyberspace and emerging technologies—particularly Artificial Intelligence (AI)—has become a new frontier of diplomatic competition. While much scholarly attention remains fixed on the established centers of digital power—the liberal-technocratic West led by the United States and Europe, and the centralized, authoritarian model exemplified by China—another narrative is steadily emerging from the Global South. Nations historically marginalized in global technological and normative frameworks are strategically repositioning themselves, aiming to negotiate a form of digital sovereignty that resists alignment with the prevailing ideological poles. Among these, India has rapidly emerged as an influential, albeit complex, actor navigating the digital divide through an increasingly visible cyber-diplomatic strategy.

India's strategy not only resonates with the historical ethos of the Non-Aligned Movement (NAM)—originating at the Bandung Conference of 1955—but reinterprets and extends these principles into the digital era (Panda, 2015; UNIDIR, 2021). Far from representing a passive stance of neutrality, this modern digital non-alignment is marked by assertive diplomatic maneuvering (Basu, 2022; Kant & Rossow, 2022), pragmatic hedging, and deliberate multilateral engagement (Lewis, 2024; Patel & Shrivastava, 2025; Bandura, McLean & Smutny, 2024; Narasimhan, 2024). India's policy initiatives, such as Digital India, the IndiaAI strategy, and the Data Empowerment and Protection Architecture (DEPA), offer clear evidence of this proactive yet deliberately balanced approach. These initiatives illustrate how digital sovereignty is strategically leveraged not merely as an internal governance framework, but as a diplomatic instrument aimed at reshaping the global norms on data governance, AI ethics, and cybersecurity standards.

The stakes of understanding this approach extend far beyond scholarly curiosity. As nations from Africa to Southeast Asia seek viable alternatives amid the intensifying Sino-American technological rivalry, India's example could become a normative template, influencing the

future digital orientation of the broader Global South. Moreover, analyzing India's cyber diplomacy through the prism of digital non-alignment offers scholars and policymakers alike a fresh theoretical and empirical lens, challenging the conventional binary paradigms that currently dominate the discourse on the global technological governance.

Through an interdisciplinary approach blending international law, critical security studies, AI governance frameworks, and diplomatic theory, this article endeavors to illuminate the strategic rationale underpinning India's digital diplomacy. Furthermore, by embedding India's policy trajectory within the wider geopolitical context, it critically assesses the potential for India's model to meaningfully influence international norms, governance structures, and diplomatic practices in cyberspace.

## The Main Digital Blocs Forming: Fragmentation, Sovereignty, and Competing Governance Models

The contemporary digital order is increasingly defined by ideological, normative, and infrastructural fragmentation. At the core of this fragmentation there is a growing divergence in state preferences over the governance of cyberspace and control over digital assets. While the liberal democracies in the West, particularly the United States and the European Union, promote an open, interoperable, and multistakeholder-based internet, a counter-model grounded in digital authoritarianism and cyber sovereignty has gained traction among states such as China and Russia (Patel & Shrivastava, 2025). These competing visions have catalyzed the emergence of distinct "digital blocs" – constellations of states aligning around normative principles, technological architectures, and policy orientations in cyberspace governance.

The liberal bloc, often aligned with the multistakeholder model, supports the unrestricted cross-border data flows, decentralised internet governance, and industry-led standard-setting. In contrast, the authoritarian bloc asserts national control over the digital infrastructure and content, codified through national laws such as China's 2017 Cybersecurity Law and Russia's 2019 Sovereign Internet Law, both of which aim to insulate their digital ecosystems from external influence (Patel & Shrivastava, 2025).

Amid these polarised digital camps, India and other countries in the Global South have sought a third path – one that neither fully adheres to the liberal openness nor embraces the authoritarian insulation. This geopolitical shift has prompted the rise of the Global South as an increasingly assertive actor in digital governance. Countries like India are advancing their own models of digital sovereignty, centred on the national control over data, infrastructure, and normative frameworks, without fully subscribing to either of the dominant models (PWonlyIAS, 2024).

India's articulation of digital sovereignty rests on three interlinked pillars: (1) economic self-determination through control over citizen-generated data; (2) strategic autonomy in resisting unequal digital trade agreements; and (3) normative positioning in multilateral forums such as the WTO and GPAI (Patel & Shrivastava, 2025; PWonlyIAS, 2024). These pillars are underpinned by a set of domestic instruments such as the Digital Personal Data Protection Act, 2023, and policy frameworks like Digital India and DEPA, which institutionalise India's aspirations for technological self-governance and normative influence (Ministry of Electronics and IT, 2025).

Thus, the formation of digital blocs cannot be reduced to binary oppositions between liberalism and authoritarianism. Rather, the emergence of the Global South introduces a pluralistic layer to this polarisation – one shaped by hybrid governance logics, asymmetric capabilities, and a desire to avoid entrapment in techno-strategic dependencies.

Figure 1 maps the major global actors across two axes—digital openness and strategic autonomy—illustrating India's unique non-aligned position relative to Western liberalism and Chinese authoritarianism. The contemporary digital landscape is characterized by an emergent tripartite fragmentation, as states coalesce around liberal, sovereign, and authoritarian models of cyber governance. James Andrew Lewis (2024) describes this phenomenon as a decline in great power cooperation—what he terms "fragmentation"—in which contending blocs promulgate divergent norms on issues ranging from data flows to incident response. In the liberal camp, coalition partners emphasize multistakeholder governance, transparency, and privacy protection; in the sovereign model, states assert data localization and national control over digital platforms; while authoritarian regimes prioritize censorship and surveillance architectures. Navigating these competing paradigms poses a core challenge for the middle powers such as India, which must reconcile its democratic commitments with the imperatives of a strategic autonomy.

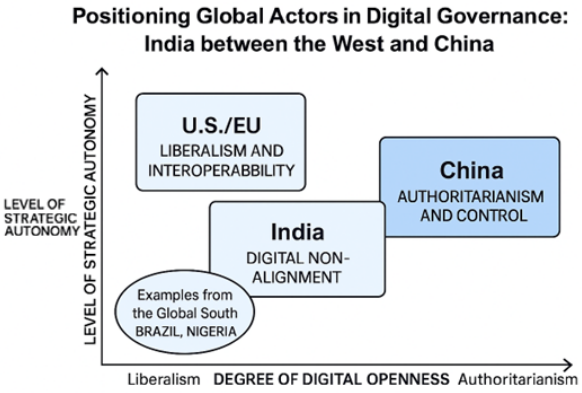


**Figure 1.** Positioning Global Actors in Digital Governance: India between the West and China

Figure 2 is a Venn diagram that shows how India strategically combines elements from both liberal and authoritarian models—such as openness and ethical AI on one side, and national sovereignty and internal control on the other—to define a hybrid digital governance posture.

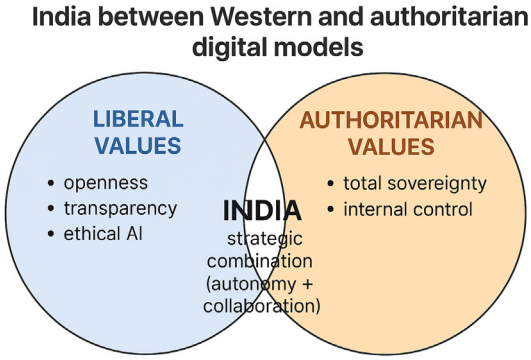


**Figure 2.** India between Western and Authoritarian Digital Models

India's positioning must also be viewed through its broader strategic competition with China. Vanshree P. Panda's edited volume on India–China relations (2015) situates the digital economic contestation within a larger struggle over resources, identity and authority in a multipolar order. Panda argues that China's state driven technological model—exemplified by the Digital Silk Road—seeks to export infrastructure and standards that reinforce Beijing's global sway, compelling New Delhi to craft parallel initiatives, such as Digital India and India Stack, to preserve its comparative advantage (Panda, 2015). Thus, India's diplomatic playbook must span both normative forums—where it champions open data and interoperable standards—and bilateral security dialogues addressing supply chain resilience and technology transfer.

## The Theory of Digital Non-Alignment: From Bandung to AI

The idea of digital non alignment adapts the Cold War principle of strategic autonomy to the cyber era. Rather than affiliating exclusively with any one block, the Global South states pursue pluralistic approaches that preserve their flexibility and hedging capacity. Bandura, McLean & Smutny (2024) provide an empirical foundation for this concept by comparing diverse models of Digital Public Infrastructure (DPI) across the Global South, from India Stack's open API architecture to Nigeria's unified identity database. They show how these platforms enable the states to engage selectively with multiple technology partners while retaining domestic control over their core data assets.

The continuity with Bandung era non alignment resides in the commitment to the sovereign choice: just as mid century Non Aligned Movement members sought to avoid superpower entanglements, today's digital non aligned actors resist the binary loyalties in cyber norms (Panda, 2015; UNIDIR, 2021; Lewis, 2024; Basu, 2022). Yet ruptures emerge from new instruments—AI ethics frameworks, cross border threat sharing mechanisms and cybercrime conventions—that did not exist in the 1950s (Jensen & Atalan, 2025; Innovation in Defence Services & Technology, 2022; Drishti IAS, 2024). This pluralism demands novel diplomatic strategies: India and its Global South peers must not only articulate an alternative normative vocabulary but also operationalize it through interoperable pilot projects and coalition based standard setting bodies (Bandura, McLean & Smutny, 2024; Smart Partnerships, 2021; Ministry of Electronics and IT, 2025).

India's approach to the cyber diplomacy and technological governance resonates with a deeper historical pattern of non-alignment in international affairs, rooted in the Bandung Conference of 1955 and institutionalized through the Cold War-era Non-Aligned Movement (NAM) (Panda, 2015; UNIDIR, 2021). The non-alignment originally sought to preserve political autonomy amidst any bipolar confrontation (Basu, 2022; Lewis, 2024). In the digital era, a parallel logic of the digital non-alignment appears to be emerging—one premised on strategic hedging, normative pluralism, and technological self-determination of states in the Global South (Bandura, McLean & Smutny, 2024; Patel & Shrivastava, 2025; Smart Partnerships, 2021).

The digital non-alignment, unlike its classical predecessor, is not merely reactive. It is proactively strategic, grounded in four rationales. First, it enables the states to preserve their freedom of maneuver in rapidly evolving domains such as AI, cyber governance, and

data trade. Second, it supports the development of the domestic technology ecosystems, insulating the national innovation from the distortions of any technological dependency (UNIDIR, 2022). Third, the digital non-alignment provides a buffer against an external coercion, such as unilateral sanctions or the extraterritorial surveillance regimes. And fourth, it allows the emerging economies to exert a regional influence, experimenting with their own their digital initiatives while remaining diplomatically agile in multilateral settings (Patel & Shrivastava, 2025).

India's model exemplifies these dynamics. Rather than subscribing fully to the open-data frameworks favoured by the OECD or to the state-centred norms of China and Russia, India has carved out a hybrid approach. This is reflected in its refusal to endorse the Osaka Declaration on Cross-Border Data Flows, its simultaneous engagement with the Global Partnership on Artificial Intelligence (GPAI) and the Shanghai Cooperation Organisation (SCO), and its proposal for modular governance through DEPA, which permits a selective adherence to digital trade rules (PWonlyIAS, 2024). Figure 3 illustrates India's response to the global digital polarization through a logic of non-alignment—combining plural forum participation, domestic DPI development, and resistance to rigid cross-border data frameworks.

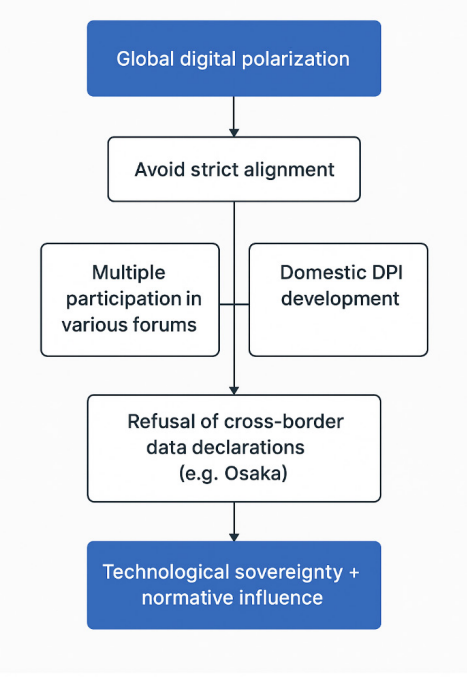


**Figure 3.** The Strategic Logic of India's Digital Non-Alignment

From a doctrinal standpoint, India has so far refrained from publicly articulating a comprehensive cyber operations doctrine. Nevertheless, its institutional architecture – spanning the Defence Cyber Agency (DCA), the National Cyber Coordination Centre (NCCC), and the MEA's Emerging Technologies Division – reflects a capacity and intent to develop cyber capabilities while avoiding an overt doctrinal alignment (UNIDIR, 2022).

In this context, the digital non-alignment should be understood less as a fixed policy and more as a fluid strategic disposition, responsive to shifts in the international normative

and technological environment. It aligns with India's broader diplomatic style: norm entrepreneurship without hegemonic ambition, rule-shaping without bloc formation, and strategic autonomy without isolationism.

Ultimately, the digital non-alignment invites a reconceptualisation of the sovereignty in the cyberspace – one that transcends Westphalian binaries and embraces multivector, layered, and interoperable sovereignties, rooted in both territorial jurisdiction and normative pluralism. As such, it represents not only a geopolitical strategy, but also a conceptual challenge to the prevailing architectures of a global cyber governance.

## INDIAN CYBER DIPLOMACY

### Participation in International Forums & geopolitical positioning

India's cyber diplomacy is marked by a deliberate multilateral engagement strategy aimed at shaping the global norms of the cyberspace governance while maintaining a strategic autonomy. India has adopted a platform-agnostic approach by participating in a range of global and regional forums that reflect varying normative and geopolitical orientations. Figure 4 highlights the key milestones in India's cyber-diplomatic strategy, from the launch of Digital India in 2015 to its growing multilateral engagement and leadership role in AI and data governance by 2025. According to UNIDIR (2022), India's involvement spans major multilateral groupings such as the United Nations (UN), BRICS, and the Shanghai Cooperation Organisation (SCO), each of which serves different strategic and normative purposes.

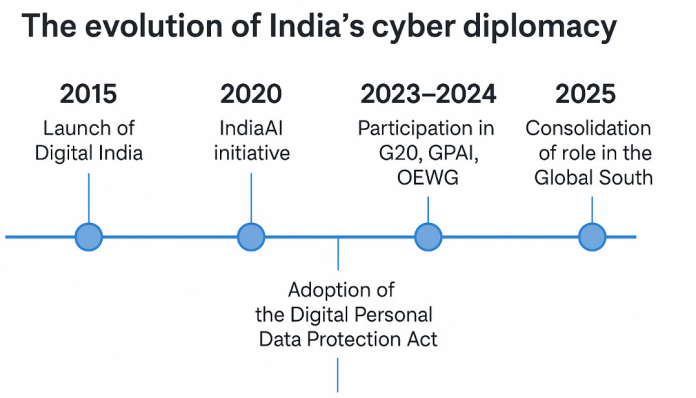


**Figure 4.** Timeline: Evolution of India's Cyber Diplomacy

At the UN level, India has pushed for recognition of state sovereignty in cyberspace and adherence to international law (UNIDIR, 2021; Basu, 2022). It has also stressed capacity building for the Global South (Bandura, McLean & Smutny, 2024; Smart Partnerships, 2021). Its proposals in OEWG include promoting a peaceful, secure, open, and cooperative ICT environment (Lewis, 2024; Patel & Shrivastava, 2025), while underscoring that cyber norms must evolve inclusively, with due regard to developmental asymmetries among states (Digital India (MeitY), 2023c; PRS Legislative Research, 2023).

Within BRICS, India advances a vision of multipolar digital governance. It supports proposals for a common BRICS framework on cybercrime and data governance (Panda, 2015; UNIDIR, 2021; Basu, 2022), emphasizing shared technological development and non-interference. In the SCO, India's engagement reflects strategic balancing—participating in cybercrime dialogues while avoiding overcommitment to the state-centric surveillance norms favored by China and Russia (Rossow, 2024; Lewis, 2024; Patel & Shrivastava, 2025).

Complementing this, the National Cyber Security Strategy (NCSS) developed by the Data Security Council of India (DSCI) calls for India's integration into international cyber regimes as both a norm entrepreneur and a responsible stakeholder. It outlines the need for India to lead in emerging technology standards, digital trade norms, and cross-border data governance, while advocating a "glocal" approach—rooted in national interest but responsive to global expectations.

India’s multilateral cyber diplomacy thereby reflects a dual imperative: projecting influence in shaping international norms while preserving digital sovereignty, in alignment with the principles of the digital non-alignment discussed earlier.

Under its 2023 G20 presidency, India advanced a normative agenda that foregrounded the digital governance as central to the inclusive growth and global stability. Amitabh Kant and Richard M. Rossow (2022) detail how India steered the G20 discussions toward commitments on cross border data flows, digital public goods and capacity building for cyber resilience. India’s emphasis on equitable access to technologies and multistakeholder collaboration signalled its intent to reshape the digital rule book in favour of the emerging economies, positioning itself as both agenda setter and bridge builder between advanced and developing members.

Parallel to the G20, India’s engagement in the Global Partnership on Artificial Intelligence (GPAI) has cemented its role in multilateral AI governance. The Ministry of Electronics & Information Technology (2023) outlines India’s contributions to GPAI working groups on responsible AI, data governance and skilling. By championing open source tools and inclusive frameworks, India has showcased its model of digital public infrastructure—embodied in India Stack—as a template for the Global South peers, thereby exporting normative principles that blend innovation with social equity.

## Strategic and Legal Initiatives – DEPA, IndiaAI, Digital India

India’s strategic hedging is further exemplified by its proactive participation in the Quad. S. L. Narasimhan (2024) reports that the Quad Foreign Ministers’ Meeting reaffirmed commitments to joint exercises, secure supply chains for emerging technologies and an Indo Pacific cybersecurity architecture. India’s concurrent cooperation with the United States, Japan and Australia underscores a dual approach: a deepening interoperability with the democratic partners while preserving the option to engage bilaterally with other major powers, thus maintaining its autonomy in a fractured security environment.

India’s cyber diplomacy is also articulated through robust domestic initiatives that serve dual functions: enhancing its internal resilience and projecting the normative leadership externally.

Figure 5 illustrates the interconnection between India's legal instruments, digital infrastructure, institutional actors, and strategic objectives—underpinning its approach to technological sovereignty and global influence.

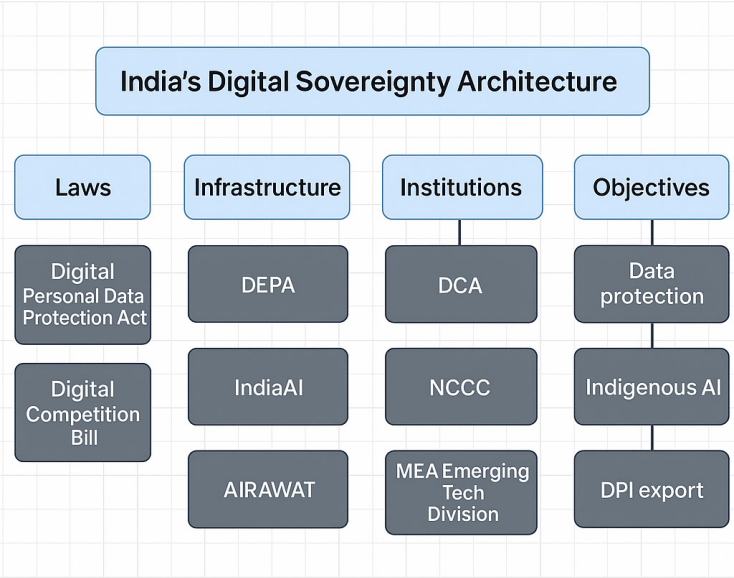


**Figure 5.** India's Digital Sovereignty Architecture

The Strategic Plan of the Department of Information Technology (DIT) defines the long-term digital transformation goals across six pillars: e-Government, e-Inclusion, e-Security, e-Learning, e-Innovation, and e-Industry. These goals are operationalised through initiatives such as State Wide Area Networks (SWAN), Common Services Centres (CSCs), and State Data Centres (SDCs), which together form the infrastructural backbone of India's e-governance and digital delivery systems.

Significantly, the Plan emphasizes (Department of Information Technology, 2011):

- Use of emerging technologies (e.g., cloud computing, green ICT)
- Data privacy and cybersecurity regulations
- Development of a national electronic repository
- Citizen-centric governance frameworks

These domestic efforts not only serve India's socio-economic development but also create a template for exportable digital governance, boosting India's credibility as a soft power in the Global South.

From a legislative standpoint, the Digital Competition Bill (DCB) marks a pivotal step in aligning India's competition law with the evolving digital realities. The DCB introduces ex-ante obligations on Systemically Significant Digital Enterprises (SSDEs), targeting behaviors like self-preferencing, tying, and bundling. While inspired by the EU's Digital Markets Act, the DCB takes a more restrained, context-sensitive approach, emphasizing the due process and proportionality (Khandelwal, 2024).

India's comprehensive approach to data governance and AI reflects a synchronized strategy across the legislative, regulatory and infrastructural domains. The Digital Personal Data Protection Bill, 2023 lays the legislative cornerstone for data sovereignty by delineating consent based processing, data fiduciary obligations and cross border transfer rules under a risk based framework (PRS Legislative Research, 2023). Crucially, the Bill mandates a dedicated Data Protection Board empowered to investigate breaches and levy penalties of up to four per cent of the global turnover, signalling a strong enforcement intent (Ikigai Law, 2023).

India's Digital Personal Data Protection Act, 2023 establishes a comprehensive consent based framework for data processing, delineating the duties of the data fiduciaries and prescribing cross border transfer protocols under a risk based approach (PRS Legislative Research, 2023). A dedicated Data Protection Board, empowered to investigate infringements and impose fines up to four per cent of a data fiduciary's global turnover, underscores the Act's robust enforcement architecture (Ikigai Law, 2023).

However, the Bill's normative contours have been critiqued for leaving expansive exemptions to government processing, which Lakshmikumaran & Sridharan Attorneys (2023) warn could undermine citizen privacy and international data interoperability. They argue that the "legitimate interests" clause, if interpreted broadly, may dilute the consent principle and introduce legal uncertainty for the cross border digital trade. Such ambiguities underscore the need for clear subsidiary rules once the Act comes into force.

Yet, the Bill's broad exemptions for government processing and the ambiguous "legitimate interests" clause have drawn criticism for potentially eroding individual privacy safeguards and complicating the international data interoperability (Lakshmikumaran & Sridharan Attorneys, 2023). Such normative gaps highlight the need for precise subsidiary rules to ensure that the Act's lofty objectives translate into effective protections.

Parallel to the data legislation, India has operationalized a multi pillar AI ecosystem under its National Program on Artificial Intelligence. This flagship initiative establishes governance structures spanning public–private partnerships, sectoral task forces and capacity building modules (Digital India (MeitY), 2023d). The Artificial Intelligence Committees & Reports repository catalogues over a dozen expert panels—ranging from ethics to industry applications—that have produced policy blueprints and draft regulations (Digital India (MeitY), 2023a).

At the infrastructural level, the PoC for AI Research, Analytics and Knowledge Dissemination Platform (AIRAWAT) provides federated access to high performance computing and model libraries, democratizing R&D capabilities across the academic and start up sectors (Digital India (MeitY), 2023b). Complementarily, the IndiaAI portal consolidates policy documents, datasets and collaboration tools into a single interface, enhancing transparency and stakeholder engagement (Digital India (MeitY), 2023c).

Together, these seven initiatives—spanning the DPDP Act's legal scaffold to IndiaAI's digital commons—exemplify India's strategic vision of technological sovereignty. By coupling robust regulatory safeguards with open, interoperable infrastructures, India aims to both fortify its domestic capacities and project normative frameworks for the global AI governance.

Complementing DEPA, India's National Program on Artificial Intelligence articulates a governance model that marries public–private partnerships with sectoral task forces to advance the AI research and application (Digital India (MeitY), 2023d). Over a dozen expert committees—spanning ethics, skilling, and industry deployment—have produced foundational reports and draft regulations, illustrating a structured approach to the AI policymaking (Digital India (MeitY), 2023a).

At the infrastructural level, the AIRAWAT platform provides federated access to high performance computing and model repositories, democratizing the R&D capabilities for academia and start ups alike (Digital India (MeitY), 2023b). In parallel, the IndiaAI portal consolidates policy documents, datasets and collaborative tools into a single interface, fostering transparency and enabling stakeholder engagement across government, industry and civil society (Digital India (MeitY), 2023c).

Together, these seven initiatives—from the DPDP Act's legal scaffold to IndiaAI's digital commons—exemplify India's dual strategy of securing the technological sovereignty domestically while exporting normative and infrastructural templates for the global AI governance.

These legal instruments showcase India's attempt to balance the market contestability with the national digital autonomy, asserting its sovereign legislative model amidst the global regulatory flux. The Competition Commission of India (CCI) retains a pivotal role, signaling India's commitment to ensuring fair play without compromising innovation or economic growth.

Crucially, India's initiatives like:

- DEPA (Data Empowerment and Protection Architecture) – enabling user consent-driven data sharing
- IndiaAI – fostering indigenous AI development with ethical safeguards
- Digital India – transforming service delivery and governance at scale

All contribute to building a legislative soft power and a techno-legal governance model that can be shared with, and adapted by, other developing nations.

In this context, India's cyber diplomacy is as much about governing internally as it is about leading externally. It operationalizes a dual axis of influence: (1) exporting a rights-based, inclusive, scalable digital framework, and (2) embedding these principles into global norm-setting forums.

## NORMATIVE AND STRATEGIC IMPLICATIONS

India's cyber diplomacy is increasingly shaped by deeper normative ambitions that go beyond technical governance. At the heart of its global engagement lies a twofold imperative: to compete for influence over international digital standards, and to assert a version of digital sovereignty that accommodates both strategic autonomy and inclusive connectivity.

## Exporting Development Models: Digital India as Soft Power

The Smart Partnerships – 2021 Report argues that India is well-positioned to act as a normative exporter of its digital governance model. The country's large-scale digitization efforts—ranging from Aadhaar to Unified Payments Interface (UPI)—are often cited as scalable, affordable, and adaptable by countries in the Global South. India's narrative positions its digital architecture not merely as a technical solution, but as a developmental model that integrates governance, inclusion, and innovation (Smart Partnerships, 2021).

Figure 6 presents a strategic pyramid which visualizes India's layered approach to digital sovereignty—built upon foundational technologies and infrastructure, consolidated through legislation, and culminating in global normative participation.

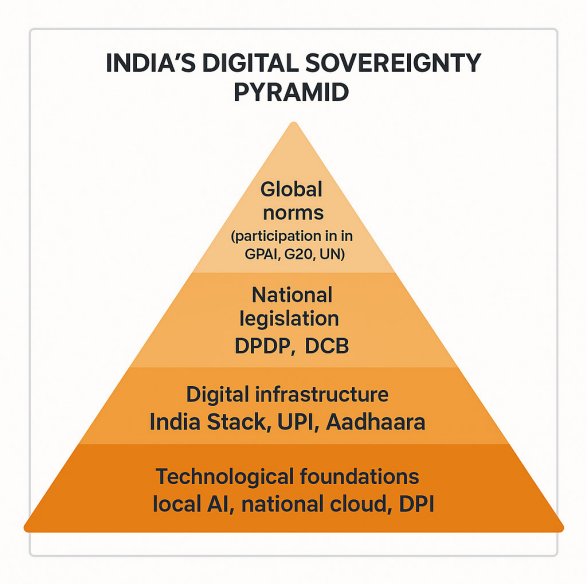


**Figure 6.** India's Digital Sovereignty Pyramid

This vision is strategically deployed in India's Digital Public Infrastructure (DPI) diplomacy. Initiatives like the G20's support for India's DPI model further validate the ambition to project "Digital India" as a transferable governance template, especially in contrast to China's surveillance-heavy model and the West's privacy-driven frameworks.

## Strategic Sovereignty vs. Globalism: A Policy Dilemma

The Policy Document by the Observer Research Foundation reflects the internal policy tensions between the strategic protectionism and the digital globalism. India's open-source and open-API policies promote the international standards and interoperability, yet the same frameworks also contain provisions that enforce localization, data sovereignty, and restrictions on cross-border data flows (Smart Partnerships, 2021).

The e-Kranti and Digital India initiatives reveal this duality. While aiming for international collaboration and the adoption of the global best practices, the policies also explicitly prioritize government control over IT infrastructure, emphasize hosting data on Government Cloud (MeghRaj), and mandate the process reengineering as a prerequisite to accessing the national digital systems.

Thus, India is both a participant in the global digital economy and a guardian of its digital boundaries—an approach that fits with its broader "strategic autonomy" doctrine in foreign policy.

Figure 7 represents a comparative table which contrasts the governance philosophies of the liberal democracies, authoritarian states, and India's hybrid model across five key dimensions: governance structure, data control, AI policy, multilateral engagement, and digital infrastructure exportation.

**Models of Digital Sovereignty: West vs. China vs. India**

| | West | China | India |
|---|---|---|---|
| Governance model | Liberal | Authoritarian | Non-aligned |
| Control over data | Technical regulations | Strict restrictions | Indigenous autonomy |
| AI policies | Ethical frameworks | National security | Holistic approach |
| Multilateral participation | Alliance building | Sovereigntist | Strategic mix |
| Export of digital infrastructure | Limited | Abundant | Emerging |

**Figure 7.** Models of Digital Sovereignty: West, China, and India

## Participatory Sovereignty in the Global Cyber Governance

In its UNIDIR "Running Single File" position, India advances the idea of a "participatory sovereignty"—a model of cyber governance where states retain sovereign control but collaborate on rule-making. India rejects both the statist, top-down model advocated by the authoritarian regimes and the West's laissez-faire digital market governance (UNIDIR, 2021).

Instead, it advocates a multistakeholder but state-anchored framework that balances rights with responsibilities. India's engagement in forums like the UNGGE and OEWG—where it calls for responsible state behavior in cyberspace—is consistent with this middle-path normative stance.

This conceptual framing aligns with India's position in other domains (e.g. climate change and trade), where it seeks equitable governance frameworks that acknowledge historical inequities while advocating differentiated responsibilities.

## Fragilities in India's IT Base: A Case for Model Diversification

The TCS Layoffs report (pwonlyias.com, 2024) highlights structural vulnerabilities in India's current IT growth model. With the automation of entry-level tech jobs and increasing competition from Global Capability Centers (GCCs), India's dependence on its traditional IT outsourcing model is showing signs of erosion.

This exposes the risks of overreliance on its legacy IT structures that are increasingly incompatible with an AI-driven global economy. As such, India's push to build and export

a new digital model—rooted in public infrastructure, citizen data ownership, and inclusive innovation—becomes not only a soft power strategy, but an economic necessity.

A model based on Digital Public Goods (DPGs), skill adaptability, and decentralized architecture might help India not just retain influence globally, but also rewire its domestic employment architecture around future-ready competencies.

## CONCLUSIONS

India's journey into cyber diplomacy reveals a nuanced redefinition of sovereignty in the digital age. No longer confined to territorial boundaries, sovereignty now encompasses control over data, technological standards, and cyber-infrastructure. The digital sphere has become an extension of the state power—yet, paradoxically, it is also a domain of shared global responsibility and contested influence. India's approach to cyber diplomacy, situated at the intersection of a strategic pragmatism and constitutional fidelity, reflects this evolving duality.

From the analysis presented in the previous chapters, it is evident that India's cyber diplomacy is fundamentally a negotiation of sovereignty—between domestic imperatives and global norms, between market liberalism and strategic protectionism, and between digital autonomy and multilateral engagement. Legal instruments such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 codify India's bid to reassert its regulatory control over cyberspace (Patel & Shrivastava, 2025). Judicial decisions, including K.S. Puttaswamy v. Union of India and Shreya Singhal v. Union of India, have entrenched privacy and free expression as digital rights, thus compelling the state to balance enforcement power with constitutional accountability (Ikigai Law, 2023).

India's dual identity—both as a developing nation with critical infrastructure vulnerabilities and a normative actor exporting its digital governance models—adds complexity to its diplomatic posture. On one hand, India champions multilateralism and sovereignty, often aligning with the Global South narratives that seek to resist the Western digital hegemony. On the other, it increasingly exports its digital public infrastructure (DPI) frameworks such as Aadhaar and UPI, transforming itself into a soft power hub in the Global Digital South (Smart Partnerships, 2021).

This duality is reflected in India's cautious stance toward global cyber norms. While participating in forums such as the UNGGE and OEWG, India resists binding international obligations like the Budapest Convention, emphasizing the need for sovereign digital frameworks that respect national jurisdiction (UNIDIR, 2021). The formulation of state responsibility in cyber operations, as explored in India's doctrinal submissions, further underscores this sovereignty-first approach (Patel & Shrivastava, 2025).

However, India's domestic challenges increasingly pressure this strategic balance. The rise of the AI threatens the traditional IT service models, as evidenced by the widespread layoffs in firms like TCS, signaling a crisis in the export-dependent digital economy (pwonlyias.com, 2024). These structural vulnerabilities justify India's pursuit of a more resilient, rights-respecting, and sovereign digital order.

Looking forward, India's cyber diplomacy will likely consolidate around four strategic axes:

1. Multilateral Norm Entrepreneurship – Leveraging its normative legitimacy in the Global South, India may increasingly shape global cyber norms by advocating inclusive governance models and capacity-building mechanisms.

2. Regulatory Sovereignty and Legal Precision – Strengthening extraterritorial claims under the DPDP Act, enforcing compliance through bodies like the Data Protection Board, and refining intermediary liability regimes to balance innovation with accountability.

3. Digital Infrastructure Exportation – Expanding India's DPI model as a counterweight to Western and Chinese digital hegemonies, positioning India as a provider of "digital public goods."

4. Constitutional Cybersecurity – Embedding digital sovereignty within a constitutional rights framework that ensures proportionality, transparency, and judicial review, thus maintaining legitimacy both at home and abroad.

Figure 8 visualizes the four strategic axes guiding India's cyber diplomacy: multilateral norm entrepreneurship, regulatory sovereignty and legal precision, digital infrastructure exportation, and constitutional cybersecurity. Together, they illustrate India's hybrid approach—balancing state sovereignty with global digital cooperation.

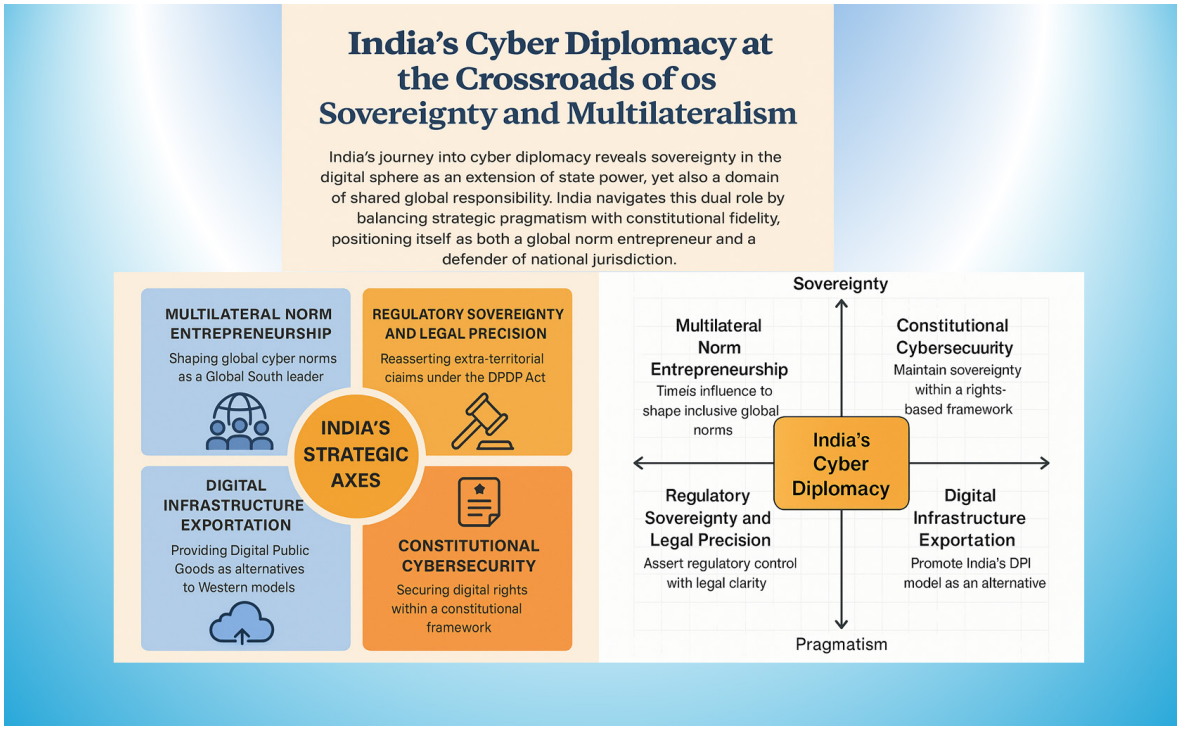


**Figure 8.** India's Cyber Diplomacy at the Crossroads of Sovereignty and Multilateralism

Ultimately, India's cyber diplomacy is not merely about securing networks—it is about defining the terms of a global digital order. It is a diplomacy of rights and rules, sovereignty and standards, ambition and caution.

As the first Global South power to engage so thoroughly with the multifaceted dimensions of the cyber governance, India is not just reacting to the fragmentation of the digital order—it is actively shaping its future contours. In an era marked by growing geopolitical fragmentation and intensified digital competition, India's cyber diplomacy emerges as a strategic and normative alternative to the dominant Western and Chinese paradigms. Rather than choosing sides in a polarized global digital order, India advances a model of "digital non-alignment," rooted in a sovereign control over data and infrastructure, but also in a global norm entrepreneurship and inclusive governance.

India—leveraging its legacy as a non-aligned power and its growing digital capabilities—is redefining the technological sovereignty in the age of AI. Through flagship initiatives such as Digital India, DEPA, and IndiaAI, and via active participation in forums like the G20, GPAI, and the UN cyber norm discussions, India positions itself as both a Global South champion and a soft power exporter of digital public infrastructure.

Offering a unique blend of regulatory autonomy, constitutional safeguards, and multilateral engagement, India's cyber diplomacy reveals a hybrid logic—one that resists binary frameworks and offers an alternative model of governance for other emerging economies. By unpacking India's strategic posture, legal instruments, and policy architecture, the article has illuminated broader transformations in the global cyber governance, while raising new questions about sovereignty, interoperability, and the future of the digital diplomacy.

## REFERENCE LIST


Bandura, R., McLean, M. & Smutny, C. (2024) *Approaches to digital public infrastructure in the Global South.* CSIS Analysis. Available at: https://www.csis.org/analysis/approaches-digital-public-infrastructure-global-south

Basu, A. (2022) *India's international cyber operations: Tracing national doctrine and capabilities*. UNIDIR. Available at: https://unidir.org/publication/indias-international-cyber-operations

Chair on India and Emerging Asia Economics, CSIS. (2024) *Rating India 2024: Key opportunities and risks*. CSIS. Available at: https://www.csis.org/events/rating-india-2024-key-opportunities-and-risks

Department of Information Technology. (2011) *Strategic plan for next five years*. Ministry of Communications & IT.

Digital India (MeitY). (2023a) *Artificial Intelligence Committees & Reports*. Available at: https://www.digitalindia.gov.in/initiative/artificial-intelligence-committees-reports/

Digital India (MeitY). (2023b) *Design, development & deployment of national AI portal* (*IndiaAI*). Available at: https://www.digitalindia.gov.in/initiative/design-development-and-deployment-of-national-ai-portal-indiaai/

Digital India (MeitY). (2023c) *Global Partnership on Artificial Intelligence*. Available at: https://www.digitalindia.gov.in/initiative/global-partnership-on-artificial-intelligence/

Digital India (MeitY). (2023d) *National Program on Artificial Intelligence*. Available at: https://www.digitalindia.gov.in/initiative/national-program-on-artificial-intelligence/

Digital India (MeitY). (2023e) *PoC for AI Research, Analytics and Knowledge Dissemination Platform* (*AIRAWAT*). Available at: https://www.digitalindia.gov.in/initiative/poc-for-ai-research-analytics-and-knowledge-dissemination-platform-airawat/

Drishti IAS. (2024) *Global Cybersecurity Index* (*GCI*) *2024 – News analysis*. Available at: https://www.drishtiias.com/daily-updates/daily-news-analysis/global-cybersecurity-index-gci-2024

DSCI. (2020) *National Cyber Security Strategy 2020 – Public Submission.* Data Security Council of India.

Hadda, K. B. (2022) *Why Indian states are important for U.S.–India ties*. CSIS. Available at: https://www.csis.org/analysis/why-indian-states-are-important-us-india-ties

IDSA Books. (2016) *India and Central Asia: The strategic dimension*. 2nd edn. Available at: https://www.idsa.in/publisher/book/india-and-central-asia-the-strategic-dimension-2

Ikigai Law. (2023) *Summary of India's Digital Personal Data Protection Act, 2023*. Available at: https://www.ikigailaw.com/article/9/summary-of-indias-digital-personal-data-protection-act-2023

Innovation in Defence Services & Technology. (2022) *India's joint doctrine for cyberspace operations: Strengthening national security in the digital age*. Available at: https://idstch.com/geopolitics/indias-joint-doctrine-for-cyberspace-operations-strengthening-national-security-in-the-digital-age/

Jensen, B. & Atalan, Y. (2025) *AI benchmarking and the future of foreign policy*. CSIS. Available at: https://www.csis.org/analysis/ai-benchmarking-and-future-foreign-policy

Kant, A. & Rossow, R. M. (2022) *India's leadership of the G20*. CSIS. Available at: https://www.csis.org/events/indias-leadership-g20

Khandelwal, P. (2024) Tying, self-preferencing and the Digital Competition Bill: A changing landscape for competition intervention? *Indian Journal of Law and Technology*, 19(2), pp. 69–84.

Krishna, J. (2024) *Locating the technology agenda in India's 2024 general election*. CSIS. Available at: https://www.csis.org/analysis/locating-technology-agenda-indias-2024-general-election

Lakshmikumaran & Sridharan Attorneys. (2023) *Analysing the Digital Personal Data Protection Bill, 2023*. Available at: https://www.lakshmisri.com/insights/articles/analysing-the-digital-personal-data-protection-bill-2023/

Lewis, J. A. (2024) *Fragmentation or like mindedness: Rethinking responsible behavior in the age of multilateralism*. CSIS. Available at: https://www.csis.org/analysis/fragmentation-or-mindedness-rethinking-responsible-behavior-age-multilateralism

Narasimhan, S. L. (2024) *Outcomes of the Quad Foreign Ministers' Meeting*. CSIS. Available at: https://www.csis.org/analysis/outcomes-quad-foreign-ministers-meeting

Panda, V. P. (ed.) (2015) *India–China relations: Politics of resources, identity and authority in a multipolar world order*. Abingdon: Routledge.

Patel, A. S. & Shrivastava, A. (2025) Digital sovereignty and state responsibility: Navigating cybersecurity challenges in India's legal landscape. *LawFoyer International Journal of Doctrinal Legal Research*, 3(1), pp. 583–613. Available at: https://lijdlr.com

Ministry of Electronics and IT (2025) *e-Governance policy initiatives under Digital India: e-Kranti, open source, cloud, and cybersecurity*. Ministry of Electronics and IT, Government of India.

PRS Legislative Research. (2023) *Digital Personal Data Protection Bill, 2023*. Available at: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

pwonlyias. (2024) *India's stand on digital sovereignty: Challenges and solutions*. Available at: https://pwonlyias.com/current-affairs/digital-sovereignty/

pwonlyias.com. (2024) *TCS layoffs: Why India's IT dream needs a wake-up call in the age of AI*. Available at: https://www.pwonlyias.com

Reinsch, W. A. & Suominen, K. (2023) *Are U.S. digital platforms facing a growing wave of ex ante competition regulation?* CSIS. Available at: https://www.csis.org/analysis/are-us-digital-platforms-facing-growing-wave-ex-ante-competition-regulation

Rossow, R. M. (2024) *U.S.–India security cooperation: Thriving through turbulence*. CSIS. Available at: https://www.csis.org/analysis/us-india-security-cooperation-thriving-through-turbulence

Smart Partnerships. (2021) *Smart partnerships and digital development: India's emerging model*. Observer Research Foundation. Available at: https://www.orfonline.org

Tomoshige, H. (2023) *The strategic convergence of the U.S.–India innovation partnership*. CSIS. Available at: https://www.csis.org/blogs/perspectives-innovation/strategic-convergence-us-india-innovation-partnership-0

UNIDIR. (2021) *India and international cyber operations: Sovereignty, strategy, and multilateralism*. Geneva: United Nations Institute for Disarmament Research. Available at: https://www.unidir.org

**Daria-Elena POPESCU** is a Master's Student in Security and Technology at the Department of International Relations and European Integration, National University of Political Studies and Public Administration (SNSPA), and a Law student at the Romanian-American University. She holds a Bachelor's degree in International Relations and European Studies from SNSPA's Faculty of Political Science and has professional experience within the Romanian Parliament, the Romanian Diplomatic Institute, and NGOs, where she coordinated projects on human rights, gender equality, and civic engagement. She has participated in multiple international conferences, and high-level training programmes, including an intensive interdisciplinary Summer School on AI and Neurosciences, with a focus on neuroimaging and brain–computer interfaces. Her fields of academic interest lie at the confluence of international relations, international law, technology and security, with a particular emphasis on the geopolitical implications of emerging technologies and on how legal frameworks, geopolitical strategies, and technological innovation shape global governance. She is particularly drawn to the tensions between state sovereignty and international obligations in times of crisis, the role of narratives—political, diplomatic, and media—in shaping public opinion and policy outcomes and the strategic relevance of cyber diplomacy and digital diplomacy in the contemporary international affairs. Her work further explores how emerging technologies—such as the artificial intelligence and brain–computer interfaces—are redefining the global security architecture, transforming the diplomatic practice, and shaping the norms of the international engagement in the digital era.