THE DIGITAL TRANSFORMATION OF INDIA'S FOREIGN POLICY: CYBER DIPLOMACY, SOVEREIGNTY AND INTERNATIONAL SECURITY

Dr. Kiran Singh, Assistant Professor, Faculty of Law,
Allahabad Degree College, University of Allahabad

ABSTRACT

This article undertakes a doctrinal and policy analysis of cyber diplomacy as an evolving instrument of Indian foreign policy, examining how international legal principles of state sovereignty, non-intervention, and use-of-force doctrines are being reinterpreted in cyberspace. It situates India's position within the contested application of customary international law to cyber operations, engaging with the Tallinn Manual 2.0's attempt to extend jus ad bellum and jus in bello frameworks to state-sponsored cyber activity, and with the International Law Commission's Draft Articles on State Responsibility as applied to cyber attribution. It draws on the International Court of Justice's reasoning in Nicaragua v. United States (1986) and Corfu Channel (1949) to interrogate the threshold for "intervention" and due diligence obligations in the digital domain. On the domestic front, it analyzes landmark Indian jurisprudence shaping cyber governance, including Justice K.S. Puttaswamy v. Union of India (2017) on informational privacy as a facet of sovereignty, Shreya Singhal v. Union of India (2015) on digital speech regulation, and the statutory architecture of the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023. The article further examines India's engagement with the UN Group of Governmental Experts and Open-Ended Working Group processes on responsible state behaviour in cyberspace, absent accession to the Budapest Convention. It argues that India's cyber diplomacy reflects a distinctive legal strategy asserting techno-sovereignty while resisting binding multilateral cyber treaties, and offers a framework for understanding how emerging powers reconcile international legal obligations with strategic autonomy in digital governance.

Keywords: cyber diplomacy, sovereignty, techno-sovereignty, jus ad bellum, attribution, data protection, India, international law.

I. Introduction

Cyberspace has, within the span of a single generation, migrated from the periphery of statecraft to its very centre. What began as a technical layer of civilian communication infrastructure is now a contested strategic domain in which states project power, gather intelligence, disrupt adversary infrastructure, and negotiate the rules of engagement through diplomatic fora. India, as one of the world's largest digital economies and the possessor of the world's biggest population of internet users, occupies a singular position in this transformation [1] simultaneously a target of persistent cyber intrusions, a champion of an alternative model of internet governance, and an aspirant to the status of a rule-shaping rather than a rule-taking power in the emerging cyber order.

This article examines the doctrinal foundations and policy contours of what may be termed India's "cyber diplomacy" the deliberate use of diplomatic, legal, and institutional instruments to advance India's interests in the governance of cyberspace, to resist the unilateral application of contested international legal norms to its detriment, and to secure recognition for a sovereignty-centric conception of digital governance. The central thesis advanced here is that India's cyber diplomacy is not merely reactive but reflects a coherent, if evolving, legal strategy: one that asserts what this article calls "techno-sovereignty" [2] while deliberately withholding accession from binding multilateral instruments most notably the Budapest Convention on Cybercrime that it perceives as encoding the normative preferences of the states that drafted them.

The analysis proceeds in three registers. First, it engages the international legal architecture within which cyber operations are increasingly, if imperfectly, regulated: the principles of sovereignty and non-intervention, the use-of-force and armed-attack thresholds under the U.N. Charter, and the customary international law of state responsibility as applied to the peculiar evidentiary problem of cyber attribution. Second, it turns inward to India's domestic constitutional and statutory framework, arguing that decisions such as *Justice K.S. Puttaswamy*

[1] See Int'l Telecomm. Union, Measuring Digital Development: Facts and Figures 2024, at 12 (2024) (documenting India's internet user base as among the largest globally).

[2] The term "techno-sovereignty" is used descriptively in this article to capture the fusion of traditional Westphalian sovereignty claims with contemporary assertions of jurisdictional and regulatory control over data, infrastructure, and platforms located within or connected to national territory. Cf. Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677, 680–82 (2015) (describing comparable trends of "data nationalism" among emerging digital powers).

v. Union of India[3] and *Shreya Singhal v. Union of India*[4], together with the Information Technology Act, 2000 [5] and the Digital Personal Data Protection Act, 2023 [6], constitute the domestic legal scaffolding upon which India's external cyber posture rests. Third, it examines India's participation in the United Nations Group of Governmental Experts ("UN GGE") and Open-Ended Working Group ("OEWG") processes, and its calculated abstention from the Budapest Convention, as evidence of a distinctive diplomatic strategy pursued by India and, more broadly, by a class of emerging digital powers seeking strategic autonomy in an area of law still very much in formation.

II. Cyber Diplomacy as an Instrument of Foreign Policy

Cyber diplomacy may be defined as the application of diplomatic resources and functions to protect national interests with respect to cyberspace, encompassing bilateral and multilateral negotiation over norms of responsible state behaviour, confidence-building measures, capacity-building assistance, and the diplomatic management of cyber incidents attributed formally or informally to other states [7]. Unlike traditional arms-control diplomacy, cyber diplomacy operates in a domain characterised by dual-use technology, private-sector ownership of critical infrastructure, and a chronic attribution deficit that complicates both deterrence and accountability.

For India, cyber diplomacy has developed along four interlocking tracks. The first is participation in UN-mandated norm-development processes, discussed in Part VI below. The second is bilateral cyber-security cooperation, exemplified by memoranda of understanding with the United States, Japan, Australia, and members of the European Union, typically focused on information-sharing, critical infrastructure protection, and capacity-building rather than binding legal obligation [8]. The third is regional engagement through fora such as the Quadrilateral Security Dialogue and the G20, where cyber-resilience of critical infrastructure has featured prominently in joint statements without generating binding commitments. The

[3]Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
[4]Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[5]Information Technology Act, No. 21 of 2000, India Code (2000).
[6]Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[7]See Barbara Marchetti & Roberto Baldoni, Cyber Diplomacy: A Conceptual Framework, in Cybersecurity in Italy: Governance, Emerging Technologies and Actors 45, 47–49 (Roberto Baldoni et al. eds., 2022) (offering a taxonomy of cyber-diplomatic functions).
[8]See Ministry of External Affairs, Government of India, India-U.S. Cyber Framework, Press Release (2016); Ministry of External Affairs, Government of India, India-Japan Cyber Security Cooperation, Press Release (2018).

fourth, and most doctrinally significant, is the deliberate abstention from binding multilateral cyber-crime instruments, preserving what Indian officials have described as "policy space" to develop an autonomous framework better suited to India's threat environment and its constitutional commitments to data localisation and law-enforcement access [9].

This four-track structure is not accidental. It mirrors, at the level of foreign policy, India's broader post-colonial commitment to "strategic autonomy" a doctrine that privileges issue-based coalition-building over binding alliance commitments [10]. Cyber diplomacy, on this account, is simply the newest terrain on which an older grand strategy is being enacted.

III. Sovereignty, Non-Intervention, and the Use of Force in Cyberspace

A. The Sovereignty Debate: Rule or Principle?

The threshold question in any assessment of cyber operations under international law is whether sovereignty operates as a binding primary rule such that any unauthorised cyber intrusion into another state's territorially-located infrastructure constitutes a violation or merely as a background principle from which more specific rules, such as the prohibition on intervention, are derived. The *Tallinn Manual 2.0*[11], the most comprehensive attempt by an International Group of Experts to restate customary international law applicable to cyber operations, reflects this very disagreement within its own commentary: a majority of the experts endorsed sovereignty as an independently enforceable rule, while a minority echoing the position later associated with certain Western state practice treated it as a principle informing, but not itself generating, an independent cause of action [12]. This unresolved debate has direct consequences for how India frames responses to intrusions against its critical infrastructure: if sovereignty is a binding rule, an unauthorised cyber operation against, for instance, Indian power-grid control systems is unlawful *per se*; if it is merely a principle, India would need to establish either an act of coercive intervention or an unlawful use of force to

[9]See Ministry of Electronics and Information Technology, Government of India, National Cyber Security Strategy 2020 (Draft) 9–11 (2020) (articulating the objective of a "sovereign and resilient" cyberspace).
[10]On strategic autonomy as an organising concept in Indian foreign policy, see generally C. Raja Mohan, Samudra Manthan: Sino-Indian Rivalry in the Indo-Pacific 211–14 (2012); Shivshankar Menon, India and Asian Geopolitics: The Past, Present 3–6 (2021).
[11]Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter Tallinn Manual 2.0].
[12]Tallinn Manual 2.0, supra note 11, r. 4 cmt. 6–10 (recording the divergence among the International Group of Experts on the status of sovereignty as a rule).

characterise the conduct as internationally wrongful.

India's own diplomatic statements have tended, consistently with the interests of a state that is more often targeted than targeting, to align with the majority position favouring sovereignty as an enforceable rule. In its national contribution to the OEWG process, India emphasised that "the principle of sovereignty and the international norms and principles that flow from it apply to State conduct of ICT-related activities," and that states must not use proxies to commit internationally wrongful acts using ICTs [13]. This position dovetails with India's domestic emphasis on data localisation and infrastructural control, examined in Part V, since a robust sovereignty rule provides the strongest available legal basis for treating extraterritorial data flows and foreign platform conduct as subject to Indian jurisdictional claims.

B. Non-Intervention and the Nicaragua Threshold

The prohibition on intervention in the internal or external affairs of another state, while related to sovereignty, is doctrinally distinct and better settled in customary international law. The International Court of Justice's judgment in *Military and Paramilitary Activities in and against Nicaragua* remains the leading authority. There, the Court held that a prohibited intervention must bear on matters in which each state is permitted, by the principle of state sovereignty, to decide freely such as the choice of a political, economic, social, and cultural system and, critically, that the intervention must be *coercive* in nature, since coercion is what "defines, and indeed forms the very essence of, prohibited intervention" [14].

Transposed to cyberspace, the *Nicaragua* coercion threshold generates significant interpretive difficulty. Cyber operations short of physical destruction election-related disinformation campaigns, the manipulation of financial-market infrastructure, or the exfiltration of sensitive government data may not obviously "coerce" a state into or away from a particular choice in the sense the Court contemplated in 1986, when it was assessing the funding and training of an armed insurgency. Commentators have accordingly debated whether a broader conception of coercion, encompassing manipulation of the informational environment on which democratic choice depends, ought to be recognised [15]. India's own experience with cross-border

[13]Ministry of External Affairs, Government of India, National Statement to the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, at 2 (2021).
[14]Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Merits, Judgment, 1986 I.C.J. 14, ¶ 205 (June 27) [hereinafter Nicaragua].
[15]See Harold Hongju Koh, International Law in Cyberspace, 54 Harv. Int'l L.J. Online 1, 3–5 (2012); Michael

disinformation and coordinated inauthentic platform activity directed at communal and electoral fault lines gives it a direct stake in this debate, and Indian statements at the OEWG have repeatedly urged that "malicious use of ICTs for interference in the internal affairs of States, including through disinformation, is a matter of serious concern" [16], without, however, committing to a specific legal test for when such interference crosses the coercion threshold a studied ambiguity that preserves India's flexibility to characterise future incidents according to their political rather than purely doctrinal significance.

C. Due Diligence and Corfu Channel

A separate but related obligation, of considerable relevance to India's frequent characterisation of cyber intrusions as emanating from or through neighbouring territory, is the due diligence obligation identified by the International Court of Justice in the *Corfu Channel* case. There, the Court held that it is "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States" [17]. Applied to cyberspace, this principle endorsed by the Tallinn Manual 2.0 as Rule 6 [18] suggests that a state which knows, or should know, that malicious cyber infrastructure operating from its territory is being used to attack another state incurs an independent obligation to take feasible measures to terminate the activity, distinct from any question of direct state attribution for the underlying attack itself.

The due diligence principle is attractive to India precisely because it lowers the evidentiary bar relative to full state responsibility: rather than needing to prove that a cyber operation is attributable to a foreign government under the ILC's Draft Articles, India need only demonstrate that the territorial state had knowledge, actual or constructive, of the harmful activity and failed to act. This is doctrinally significant given the persistent difficulty of attributing sophisticated intrusion campaigns frequently associated in threat-intelligence reporting with state-linked advanced persistent threat groups operating from India's immediate neighbourhood to a specific state actor with the degree of certainty international law traditionally demands [19]. A due diligence framing allows India to press claims of territorial

N. Schmitt, "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law, 54 Va. J. Int'l L. 697, 711–15 (2014).

[16]Ministry of External Affairs, Government of India, Statement at the UN Open-Ended Working Group on ICTs, 2 (Dec. 2021).

[17]Corfu Channel (U.K. v. Alb.), Merits, 1949 I.C.J. 4, 22 (Apr. 9) [hereinafter Corfu Channel].

[18]Tallinn Manual 2.0, supra note 11, r. 6.

[19]Compare Tallinn Manual 2.0, supra note 11, r. 15 cmt. 6 (noting the "clear and convincing evidence" standard favoured by several Experts), with Nicaragua, supra note 14, ¶ 109 (applying an "effective control" test for attribution of non-state actor conduct).

responsibility without having to clear the higher bar of direct state attribution a strategic as much as doctrinal preference.

D. Tallinn Manual 2.0: Jus ad Bellum and Jus in Bello

The most ambitious extension of existing international law to cyberspace is the Tallinn Manual 2.0's treatment of the *jus ad bellum* and *jus in bello* frameworks. On the former, the Manual accepts that a cyber operation may constitute a "use of force" within the meaning of Article 2(4) of the U.N. Charter [20] where its scale and effects are comparable to those of a kinetic operation that would qualify as such the so-called "scale and effects" test derived from the Court's dicta in *Nicaragua*[21]. A still smaller category of cyber operations, those causing effects analogous to an armed attack, may trigger the right of self-defence under Article 51 [22]. On the latter, the Manual extends the principles of distinction, proportionality, and precaution governing armed conflict to cyber means and methods of warfare, treating civilian data and civilian cyber infrastructure as protected objects in most circumstances [23].

India has neither formally endorsed nor rejected the Tallinn framework, a posture consistent with its broader ambivalence toward instruments produced without the direct participation of the Global South. India was not represented among the International Groups of Experts that produced either the original Tallinn Manual or its 2017 successor, a fact frequently noted by Indian commentators as evidence of the project's limited claim to reflect universal customary international law rather than the preferences of NATO-aligned states [24]. India's preference has instead been to channel its views through the UN GGE and OEWG processes, discussed in Part VI, which whatever their limitations offer universal state participation and therefore a stronger claim to generating or reflecting customary international law through consistent and general state practice.

IV. Attribution and State Responsibility

The customary international law of state responsibility, substantially codified in the

[20]U.N. Charter art. 2, ¶ 4.
[21]Tallinn Manual 2.0, supra note 11, r. 69 & cmt. 8–9 (adopting the scale-and-effects approach); see also Nicaragua, supra note 14, ¶¶ 191, 195.
[22]U.N. Charter art. 51; Tallinn Manual 2.0, supra note 11, r. 71.
[23]Tallinn Manual 2.0, supra note 11, rr. 92–97, 113.
[24]See Arun Mohan Sukumar, Midnight's Machines: A Political History of Technology in India 214–17 (2019) (critiquing the Euro-Atlantic provenance of the Tallinn process).

International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts [25], supplies the analytical scaffolding for determining when a cyber operation conducted by a non-state actor may nonetheless be attributed to a state. Article 8 of the Draft Articles provides that conduct is attributable to a state where the non-state actor is in fact acting on the instructions of, or under the direction or control of, that state [26]. The precise degree of control required remains contested: the International Court of Justice in *Nicaragua* applied a demanding "effective control" standard, requiring control over the specific operations in the course of which the alleged violations occurred [27], whereas the International Criminal Tribunal for the former Yugoslavia, in *Prosecutor v. Tadić*, endorsed a lower "overall control" threshold for the purpose of characterising the nature of an armed conflict [28]. The Tallinn Manual 2.0's International Group of Experts, addressing this divergence directly in the cyber context, ultimately favoured the stricter *Nicaragua* standard, while acknowledging its practical difficulty of satisfaction where cyber proxies operate with plausible deniability [29].

The practical consequence of this high attribution threshold, combined with the technical difficulty of establishing the provenance of a cyber intrusion with legally cognisable certainty, is what commentators have termed the "attribution problem" the gap between the political confidence with which states publicly attribute cyber incidents (often on the basis of classified technical indicators, geopolitical inference, and pattern-of-life analysis) and the higher evidentiary standard international adjudicatory bodies would in principle demand [30]. India's official practice reflects a cautious approach to this problem: government statements following major cyber incidents affecting Indian entities have typically stopped short of formal state attribution, preferring diplomatic protest and technical remediation, a pattern consistent with the broader tendency of states to attribute cyber operations through political rather than judicial channels [31]. This restraint is doctrinally prudent premature or legally unsupported attribution risks itself constituting an internationally wrongful act if later shown to be mistaken but it also limits India's ability to invoke the law of countermeasures, which under Article 22 of the Draft

[25]Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 26 (2001) [hereinafter ILC Draft Articles].
[26]ILC Draft Articles, supra note 25, art. 8.
[27]Nicaragua, supra note 14, ¶ 115.
[28]Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶¶ 116–45 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).
[29]Tallinn Manual 2.0, supra note 11, r. 17 cmt. 5–8.
[30]See Kristen E. Eichensehr, The Law and Politics of Cyberattack Attribution, 67 UCLA L. Rev. 520, 526–30 (2020).
[31]See Press Trust of India, India Flags Cyber Intrusion Concerns at Bilateral Talks Without Naming State Actor, (2022) (illustrative of the pattern of diplomatic rather than judicial attribution).

Articles is available only in response to an internationally wrongful act properly attributed to the responsible state [32].

V. India's Domestic Constitutional and Statutory Architecture

India's external cyber diplomacy cannot be understood in isolation from its domestic constitutional and statutory framework, which supplies both the normative justification and the institutional capacity for the sovereignty claims India advances internationally. Three developments are of particular significance: the constitutional recognition of informational privacy in *Puttaswamy*; the reading-down of intermediary liability and speech restrictions in *Shreya Singhal*; and the statutory architecture comprising the Information Technology Act, 2000, as amended, and the Digital Personal Data Protection Act, 2023.

A. Puttaswamy: Privacy as a Facet of Sovereignty

In *Justice K.S. Puttaswamy v. Union of India*, a nine-judge bench of the Supreme Court of India unanimously held that the right to privacy is intrinsic to the right to life and personal liberty guaranteed under Article 21 of the Constitution, and that informational privacy the individual's interest in controlling the dissemination of personal data is a core facet of this right [33]. While *Puttaswamy* is conventionally analysed as a domestic constitutional-rights decision, this article argues that it carries an underappreciated external dimension: by constitutionalising informational self-determination, the judgment furnished the state with a constitutional mandate to regulate the cross-border flow of Indian citizens' data, since any statutory data-localisation or cross-border transfer regime can now be defended as necessary to secure a fundamental right rather than merely as an exercise of ordinary legislative or executive discretion [34]. In this sense, *Puttaswamy* operates as the domestic constitutional analogue to the international law principle of sovereignty over data infrastructure: it recasts the protection of Indian citizens' data as a matter of constitutional right that state cyber diplomacy is obliged to defend, rather than a mere administrative convenience open to negotiation away in trade or digital-governance fora.

---

[32] ILC Draft Articles, supra note 25, art. 22; see also Tallinn Manual 2.0, supra note 11, r. 20 cmt. 3 (noting that countermeasures require attribution to a reasonable degree of certainty, though not necessarily to a criminal-law standard).

[33] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 3, 297–99 (India) (per Chandrachud, J.).

[34] See Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future 88–91 (2018) (linking Puttaswamy to the subsequent data-localisation debate).

B. Shreya Singhal: The Limits of Digital Speech Regulation

In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the Information Technology Act, 2000, which criminalised the sending of "grossly offensive" or "menacing" information by computer, as unconstitutionally vague and disproportionate, holding that it fell outside the reasonable restrictions on free speech permitted under Article 19(2) of the Constitution [35]. The Court, however, upheld Section 69A, which empowers the government to block public access to online content on specified grounds including national security and public order, subject to procedural safeguards [36].

The doctrinal significance of *Shreya Singhal* for cyber diplomacy lies in this dual holding: it disciplines the state's power to criminalise online expression while simultaneously legitimating a structured content-blocking regime justified by reference to sovereignty and national-security concerns. This combination allows India to present its domestic internet-governance model internationally as rights-respecting since the judiciary has demonstrated a willingness to strike down overbroad speech restrictions while retaining, and indeed constitutionally endorsing, an executive blocking power that foreign platforms operating in India must accommodate. It is precisely this blend of constitutional legitimacy and sovereign control that underwrites India's international insistence, echoed in its OEWG statements, that the regulation of harmful online content is a matter of domestic jurisdiction to be exercised consistently with, but not subordinated to, international human-rights discourse [37].

C. The Information Technology Act, 2000

The Information Technology Act, 2000 remains the principal statutory instrument governing cyber activity in India, addressing electronic contracts and signatures, computer-related offences, and, through Sections 43A and 72A, civil liability for the negligent handling of sensitive personal data [38]. Of particular relevance to cyber diplomacy are Sections 69 and 69A, which empower the central government to intercept, monitor, or decrypt information, and to block public access to information, respectively, on grounds including the sovereignty and

[35]Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1, ¶¶ 78, 83 (India).
[36]Id. ¶¶ 97–99 (upholding the constitutionality of Section 69A and the accompanying Blocking Rules).
[37]See Ministry of External Affairs, Government of India, National Statement to the Open-Ended Working Group, supra note 13, at 4.
[38]Information Technology Act, No. 21 of 2000, §§ 43A, 66, 69, 69A, 72A, India Code (2000).

integrity of India, the security of the state, and friendly relations with foreign states [39]. These provisions operationalise, at the level of ordinary legislation, the sovereignty claims India advances internationally: they assert plenary jurisdiction over data and content accessible within Indian territory irrespective of the location of the hosting server or the nationality of the intermediary, a jurisdictional posture that has repeatedly placed India in tension with foreign technology companies and, by extension, with the states in which those companies are headquartered [40].

D. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 represents the culmination of nearly a decade of legislative deliberation following *Puttaswamy*, and it recalibrates India's earlier, more restrictive data-localisation proposals into a comparatively liberal cross-border transfer regime: rather than requiring mirror-copies of personal data to be stored within India, as earlier draft bills had proposed, the 2023 Act permits transfer of personal data to any country or territory outside India except those specifically restricted by central government notification a "negative list" or blacklist approach [41]. The Act also establishes a Data Protection Board with powers to investigate breaches and impose significant financial penalties, and it retains broad governmental exemptions for processing in the interests of sovereignty, integrity, and security of the state [42].

The shift from a mandatory-localisation model to a negative-list cross-border transfer regime is significant for cyber diplomacy because it recalibrates, without abandoning, India's sovereignty claim. Data localisation in its strong form had been a source of considerable friction in India's trade and digital-economy negotiations, including within the G20 and in bilateral talks with the United States and the European Union, each of which had raised concerns regarding the compatibility of strict localisation mandates with the free flow of data underlying digital trade [43]. The 2023 Act's more permissive default, retaining only a residual and government-controlled power to restrict transfers to specific jurisdictions, allows India to

[39]Id. §§ 69(1), 69A(1).
[40]See generally Chinmayi Arun, Rebalancing Regulation of Speech: Hyper-Local Content on Global Web-Based Platforms, 120 Mich. L. Rev. Online 1, 6–9 (2021) (discussing extraterritorial tensions generated by India's content-blocking framework).
[41]Digital Personal Data Protection Act, No. 22 of 2023, § 16, India Code (2023).
[42]Id. §§ 17(2), 27–28 (governmental exemptions and Data Protection Board powers, respectively).
[43]See Anupam Chander, The Coming North-South Divide in Data Governance, 116 AJIL Unbound 152, 154–56 (2022) (situating India's data-localisation debate within broader North-South tensions in digital trade governance).

participate more fully in digital trade diplomacy while preserving, through the broad state-security exemptions and the residual blacklist power, the core sovereign prerogative to intervene in data flows when strategic considerations so require. This is techno-sovereignty recalibrated for commercial viability rather than techno-sovereignty abandoned.

VI. India's Engagement with the UN GGE and OEWG Processes

Since 2004, the United Nations General Assembly has convened successive Groups of Governmental Experts to examine developments in the field of information and telecommunications in the context of international security. The 2015 GGE report, endorsed by consensus and subsequently welcomed by the General Assembly, articulated eleven voluntary, non-binding norms of responsible state behaviour, together with an affirmation significant for the sovereignty debate examined in Part III that international law, and in particular the U.N. Charter, applies to state conduct in cyberspace [44]. Among the norms endorsed were commitments that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs a direct extension of the *Corfu Channel* due diligence principle and that states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure [45].

The consensus achieved in 2015 fractured at the subsequent 2016–2017 GGE, which failed to agree on a final report, largely over disagreement between states favouring an explicit statement on the applicability of the law of countermeasures and the right of self-defence in cyberspace, and states including Russia and China, though India's position was more nuanced resistant to language that might be read as legitimating unilateral, forcible responses to cyber incidents [46]. This breakdown catalysed the parallel establishment, at Russia's initiative, of the Open-Ended Working Group, open to the full UN membership rather than a select group of experts, running alongside a continuing (US-initiated) GGE track.

India has participated actively in both tracks, generally supporting the applicability of existing international law to cyberspace while resisting calls, principally from Western states, for a new binding cyber-specific treaty and resisting, equally, calls from Russia and allied states for a

[44]Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Rep., U.N. Doc. A/70/174, ¶¶ 13, 26–28 (July 22, 2015).
[45]Id. ¶ 13(c), (f).
[46]See Michael Schmitt & Liis Vihul, International Cyber Law Politicized: Introduction to a Symposium on the UN GGE's Failure to Advance Cyber Norms, Just Security (June 30, 2017).

wholly new UN convention on information security that critics view as a vehicle for content-control and information-sovereignty claims inconsistent with a multi-stakeholder internet model [47]. The OEWG's 2021 Final Substantive Report, adopted by consensus, reaffirmed the eleven voluntary norms and the applicability of international law, while establishing a further, permanent OEWG mechanism (2021–2025) to continue norm elaboration [48]. India's consistent preference for this universal-membership, consensus-based, non-binding process over both the expert-driven Tallinn approach and binding treaty proposals reflects a considered judgment that India's interests are better served by norm elaboration that preserves flexibility of interpretation and application than by rigid treaty text that could later constrain India's own conduct or invite external scrutiny of its domestic cyber-governance choices.

VII. The Budapest Convention Question

The Council of Europe's Convention on Cybercrime, concluded at Budapest in 2001, remains the only binding multilateral treaty specifically addressing cybercrime, harmonising substantive offences and establishing a framework for expedited mutual legal assistance and cross-border evidence-sharing among states parties [49]. Although open to accession by non-European states, and although a number of India's international partners are parties, India has consistently declined to accede.

India's stated objections are threefold. First, India was not party to the Convention's negotiation, and objects, as a matter of principle, to acceding to a treaty text it had no role in drafting a concern that echoes India's ambivalence toward the Tallinn Manual discussed in Part III [50]. Second, Article 32(b) of the Convention, permitting a party to access stored computer data located in another party's territory without prior authorisation from that party in specified circumstances, has been read by Indian officials as posing a risk to Indian data sovereignty by permitting unilateral cross-border data access without a corresponding mutual legal assistance request [51]. Third, India has expressed a preference for a UN-negotiated instrument with

[47]See Ministry of External Affairs, Government of India, Statement at the Open-Ended Working Group, First Substantive Session, at 2–3 (2019).
[48]Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Rep., U.N. Doc. A/AC.290/2021/CRP.2, ¶¶ 5, 9–12 (Mar. 10, 2021).
[49]Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 [hereinafter Budapest Convention].
[50]See Ministry of Electronics and Information Technology, Government of India, Response to Parliamentary Question No. 2439, Rajya Sabha (2018) (setting out India's stated reasons for non-accession).
[51]Budapest Convention, supra note 49, art. 32(b); see also Council of Europe, Cybercrime Convention Committee, T-CY Guidance Note on Article 32, at 3–4 (2014) (acknowledging continuing disagreement among

universal, rather than regional-organisation-led, provenance, a preference that has now found partial expression in the negotiation, under UN General Assembly mandate, of a new international convention on countering the use of ICTs for criminal purposes, concluded in substantially final form in 2024 [52].

India's engagement with the negotiation of this new UN cybercrime convention, while continuing to withhold accession from Budapest, illustrates the article's central argument with particular clarity. India is not opposed to binding cyber-crime cooperation as such indeed, it has actively participated in shaping the new UN instrument's provisions on electronic evidence-sharing and safeguards but it insists on binding commitments being generated through a process in which it has participated as a founding negotiator rather than a subsequent accession candidate. Sovereignty, in this framing, attaches not only to substantive jurisdictional claims but to the procedural legitimacy of the norm-creation process itself.

VIII. Techno-Sovereignty as India's Strategic Doctrine

Drawing together the international and domestic strands examined above, this article argues that India's cyber diplomacy is best understood not as an ad hoc collection of positions but as the expression of a coherent strategic doctrine of techno-sovereignty, comprising four propositions. First, existing international law the U.N. Charter, the customary law of state responsibility, and the principles articulated in *Nicaragua* and *Corfu Channel* is applicable to cyberspace and requires no new binding treaty to achieve applicability, a position that avoids the risk of a new treaty regime being negotiated primarily among, and reflecting the interests of, more technologically advanced states. Second, sovereignty operates as a binding primary rule rather than a mere principle, maximising India's ability to characterise unauthorised foreign cyber activity affecting Indian territory as internationally wrongful [53]. Third, domestic constitutional and statutory law *Puttaswamy*, *Shreya Singhal*, the IT Act, and the DPDP Act should be read as mutually reinforcing instruments that constitutionalise state control over data and content within Indian territory, providing the domestic legal predicate for India's external sovereignty claims. Fourth, and finally, new binding multilateral obligations should be

parties on the scope of Article 32(b)).

[52]G.A. Res. 74/247, U.N. Doc. A/RES/74/247 (Dec. 27, 2019) (mandating negotiation of a comprehensive international convention on countering the use of ICTs for criminal purposes); U.N. Ad Hoc Comm. to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Rep., U.N. Doc. A/AC.291/22 (2024).

[53]See supra Part III.A.

accepted only where India participates in their negotiation from the outset, as with the new UN cybercrime convention, rather than through accession to instruments such as Budapest whose terms were settled without Indian input.

This doctrine is not without internal tension. A sovereignty-maximalist international law position sits uneasily alongside the DPDP Act's comparatively liberal cross-border data-transfer default, examined in Part V.D, which was adopted substantially in response to the commercial interests of India's own burgeoning digital economy and export-oriented information-technology services sector. Similarly, India's simultaneous advocacy for a multi-stakeholder model of internet governance resisting the state-centric, content-control model advanced by Russia and China at the OEWG sits in some tension with the broad content-blocking powers upheld domestically in *Shreya Singhal*. These tensions are not evidence of doctrinal incoherence, however, but rather of the pragmatic, interest-balancing character of techno-sovereignty as actually practised: India calibrates the intensity of its sovereignty claims to the specific issue-area maximalist on state security and law-enforcement access, more accommodating on commercial data flows and platform governance in a manner functionally similar to the issue-based coalition-building that has long characterised Indian diplomacy in trade and other multilateral fora [54].

IX. Toward a Framework for Emerging Powers in Digital Governance

India's experience offers a generalisable, if provisional, framework for understanding how other emerging and middle powers reconcile international legal obligation with strategic autonomy in digital governance. Three features of the Indian approach appear transferable. First, the preference for universal-membership, consensus-based norm-elaboration processes (the UN GGE/OEWG model) over either exclusive expert-led restatements (Tallinn) or regional treaty regimes negotiated without the state's participation (Budapest) reflects a more general strategy available to states that were not present at the drafting table of earlier international legal instruments: to invest diplomatic capital in newer, more inclusive fora precisely because doing so allows a state to shape rather than merely receive the resulting norms.

Second, the deliberate pairing of a maximalist international sovereignty claim with a

[54]Cf. Amrita Narlikar, India Rising: Responsible to Whom?, 89 Int'l Aff. 595, 598–602 (2013) (describing India's issue-based, coalition-dependent negotiating style in multilateral trade diplomacy).

domestically legitimated, rights-inflected statutory and constitutional framework allows a state to answer the charge of authoritarian digital control with reference to its own constitutional courts. India's ability to point to *Puttaswamy*'s privacy holding and to the partial speech-protective outcome in *Shreya Singhal* provides a democratic-legitimacy defence for sovereignty claims that, if advanced by a state lacking comparable independent judicial review, might more readily be characterised internationally as digital authoritarianism. Third, the calibration of sovereignty intensity by issue-area strict on security and law-enforcement access, permissive on commercial data flows allows emerging powers to pursue trade and investment integration in the digital economy without appearing to abandon foundational sovereignty commitments, addressing what has been described elsewhere as the tension between data sovereignty and the economic benefits of cross-border data flows [55].

This framework should not be mistaken for a claim that India's approach is optimal or that it resolves the underlying doctrinal uncertainties examined in Parts III and IV. The scale-and-effects test for cyber uses of force, the appropriate standard of attribution, and the precise content of the due diligence obligation remain genuinely contested as a matter of positive international law, and India's advocacy for particular interpretations reflects national interest as much as legal conviction a feature India shares with every other state active in these debates. What the Indian experience does illustrate is that emerging powers need not choose between full participation in binding multilateral cyber-governance instruments and complete abstention from international legal engagement; a middle path of active norm-shaping within non-binding, universal-membership processes, coupled with selective and carefully sequenced treaty participation, is available and has been substantially exploited by India over the past decade.

X. Conclusion

This article has argued that India's cyber diplomacy, examined across its international and domestic legal dimensions, reflects a coherent strategic doctrine of techno-sovereignty: an insistence on the applicability of existing international law to cyberspace, a preference for sovereignty as a binding primary rule, the deployment of Indian constitutional jurisprudence and statutory reform as domestic legitimation for external sovereignty claims, and a calculated,

[55] See Chander, supra note 43, at 156–58 (identifying this tension as a defining feature of the emerging North-South divide in digital-trade governance).

issue-differentiated approach to binding multilateral commitment. Whether this doctrine will prove durable as the OEWG's mandate continues through 2025 and as the new UN cybercrime convention moves toward entry into force remains to be seen. What can be said with greater confidence is that India's approach offers a distinctive and analytically tractable case study of how a major emerging power is seeking to reconcile the universalist aspirations of international law with the particularist demands of national security and digital-economic strategy a reconciliation that will, in one form or another, have to be attempted by every state as cyberspace continues its transformation from a technical afterthought into a central theatre of contemporary statecraft.

Bibliography

Cases

Corfu Channel (U.K. v. Alb.), Merits, 1949 I.C.J. 4 (Apr. 9).

Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).

Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Merits, Judgment, 1986 I.C.J. 14 (June 27).

Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

Constitutional Provisions and Statutes

Constitution of India art. 19(2), art. 21.

Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

Information Technology Act, No. 21 of 2000, India Code (2000).

Treaties and International Instruments

Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (Budapest Convention).

U.N. Charter.

United Nations and Institutional Documents

Council of Europe, Cybercrime Convention Committee, T-CY Guidance Note on Article 32 (2014).

G.A. Res. 74/247, U.N. Doc. A/RES/74/247 (Dec. 27, 2019).

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Rep., U.N. Doc. A/70/174 (July 22, 2015).

Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10 (2001).

Open-Ended Working Group on Developments in the Field of Information and

Telecommunications in the Context of International Security, Final Substantive Rep., U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021).

U.N. Ad Hoc Comm. to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Rep., U.N. Doc. A/AC.291/22 (2024).

Government and Official Documents (India)

Ministry of Electronics and Information Technology, Government of India, National Cyber Security Strategy 2020 (Draft) (2020).

Ministry of Electronics and Information Technology, Government of India, Response to Parliamentary Question No. 2439, Rajya Sabha (2018).

Ministry of External Affairs, Government of India, India-Japan Cyber Security Cooperation, Press Release (2018).

Ministry of External Affairs, Government of India, India-U.S. Cyber Framework, Press Release (2016).

Ministry of External Affairs, Government of India, National Statement to the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 (2021).

Ministry of External Affairs, Government of India, Statement at the Open-Ended Working Group, First Substantive Session (2019).

Ministry of External Affairs, Government of India, Statement at the UN Open-Ended Working Group on ICTs (Dec. 2021).

Press Trust of India, India Flags Cyber Intrusion Concerns at Bilateral Talks Without Naming State Actor (2022).

Books, Articles, and Other Secondary Sources

Chinmayi Arun, Rebalancing Regulation of Speech: Hyper-Local Content on Global Web-Based Platforms, 120 Mich. L. Rev. Online 1 (2021).

Anupam Chander, The Coming North-South Divide in Data Governance, 116 AJIL Unbound 152 (2022).

Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677 (2015).

Kristen E. Eichensehr, The Law and Politics of Cyberattack Attribution, 67 UCLA L. Rev. 520

(2020).

Int'l Telecomm. Union, Measuring Digital Development: Facts and Figures 2024 (2024).

Harold Hongju Koh, International Law in Cyberspace, 54 Harv. Int'l L.J. Online 1 (2012).

Barbara Marchetti & Roberto Baldoni, Cyber Diplomacy: A Conceptual Framework, in Cybersecurity in Italy: Governance, Emerging Technologies and Actors 45 (Roberto Baldoni et al. eds., 2022).

Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (2018).

Shivshankar Menon, India and Asian Geopolitics: The Past, Present (2021).

C. Raja Mohan, Samudra Manthan: Sino-Indian Rivalry in the Indo-Pacific (2012).

Amrita Narlikar, India Rising: Responsible to Whom?, 89 Int'l Aff. 595 (2013).

Michael N. Schmitt, "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law, 54 Va. J. Int'l L. 697 (2014).

Michael Schmitt & Liis Vihul, International Cyber Law Politicized: Introduction to a Symposium on the UN GGE's Failure to Advance Cyber Norms, Just Security (June 30, 2017).

Arun Mohan Sukumar, Midnight's Machines: A Political History of Technology in India (2019).

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed., 2d ed. 2017).