SOVEREIGNTY IN THE DIGITAL REALM: INDIA'S LEGAL FRAMEWORK ON CYBER-DETERRENCE, ARTIFICIAL INTELLIGENCE GOVERNANCE, AND INTERNATIONAL LAW

Mohammad Iqbal Mohammad Kamil Dalal, Haveli Institute of Legal Studies and Research

ABSTRACT

This research paper critically evaluates the legal, strategic, and normative architecture governing India's digital sovereignty amid rapidly escalating cyber warfare and autonomous artificial intelligence (AI) integration. As the global security paradigm shifts from physical borders to domain-agnostic cyber operations, traditional public international law norms specifically state sovereignty, non intervention under Article 2(4) of the UN Charter, and the law of armed conflict (jus ad bellum and jus in bello) face severe stress. Operating at the intersection of domestic constitutional imperatives and international jurisprudence, India navigates a complex multi-alignment posture. This paper examines India's domestic legislative landscape, including the Information Technology Act 2000, the Digital Personal Data Protection Act 2023, and emerging AI governance directives, against international standards such as the Tallinn Manual 2.0 and UN GGE norms. Through a doctrinal and comparative legal methodology, the study analyzes India's counter-offensive cyber posture, state responsibility under customary international law, and algorithmic governance challenges. It identifies institutional gaps in cross-border attribution, civilian data protection during hybrid conflicts, and autonomous weapon targeting. Finally, the paper offers concrete legal and diplomatic recommendations to strengthen India's cyber-deterrence operationality while safeguarding global digital peace and human rights.

Keywords: Digital Sovereignty, Cyber-Deterrence, Artificial Intelligence, Public International Law, State Responsibility.

1. INTRODUCTION

The twenty-first century global order is undergoing an unprecedented structural transition driven by the virtualization of state power. As cyberspace and artificial intelligence (AI), systems mature from auxiliary civilian tools into foundational instruments of national defense, economic power, and geopolitics, the concept of state sovereignty has expanded beyond geographic land, sea, air, and outer space boundaries. The "digital realm" encompassing physical undersea fiber cables, logical networking protocols, cloud architectures, and cognitive AI algorithms is now a primary domain of inter-state competition, espionage, and warfare.[1]

For the Republic of India, the imperative of digital sovereignty is both urgent and complex. As the world's most populous democracy and a leading digital economy powered by extensive national infrastructure such as the Aadhaar biometric identity stack, Unified Payments Interface (UPI), and critical energy grids India faces continuous targeted cyber threats from hostile state and non-state actors. Border conflicts along the Line of Actual Control (LAC) are increasingly accompanied by asymmetric cyber offensives aimed at critical national infrastructure (CNI), power distribution grids, and military communication systems.[2] Concurrently, the proliferation of generative and dual-use AI frameworks introduces risks regarding algorithmic bias, deepfake-driven cognitive warfare, autonomous targeting, and foreign electoral interference.

In response, Indian statecraft has adopted a policy of proactive digital sovereignty. Unlike the unconstrained data extraction model of Western technological corporations or the strict state control of authoritarian firewalls, India pursues a model balancing domestic data protection, strategic autonomy, technological self-reliance (*Atmanirbhar Bharat*), and active participation in international law-making.[3] However, this strategic posture creates friction with established public international law frameworks. Treaties governing armed conflict and state responsibility such as the UN Charter and Geneva Conventions were drafted for physical battlefields and struggle to address sub-threshold cyber operations, autonomous algorithmic targeting, and attribution challenges.

This paper examines India's legal and strategic positioning within the global digital realm. It evaluates how India navigates the dual imperatives of asserting sovereign cyber deterrence and shaping international legal norms governing cyberspace and artificial intelligence.

2. RESEARCH METHODOLOGY

This study employs a doctrinal and comparative legal methodology, integrated with qualitative state-practice analysis. The legal research evaluates primary and secondary legal sources according to the Oxford Standard for Citation of Legal Authorities (OSCOLA).

The primary sources analyzed include:

Domestic Statutory and Policy Frameworks: The Constitution of India 1950;

1. Information Technology Act 2000 (and 2008 Amendments); Digital Personal Data Protection Act 2023; National Cyber Security Policy 2013; and NITI Aayog's National Strategy for Artificial Intelligence.

2. **International Legal Treaties and Instruments:** Charter of the United Nations 1945; Geneva Conventions of 1949 and Additional Protocols; Statute of the International Court of Justice (ICJ); and UN General Assembly Resolutions on Developments in the Field of Information and Telecommunications.

3. **Soft Law and Customary Reports:** The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations; Reports of the UN Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG); and draft provisions of the International Law Commission (ILC) on State Responsibility for Internationally Wrongful Acts.

The analytical framework applies public international law principles specifically sovereignty (*dominium* and *imperium*), non-intervention, due diligence, and the law of armed conflict to India's declared cyber security policies and military doctrines. Comparative legal reference is made to cyber legal frameworks across the United States, European Union, and China to assess India's positioning in the international legal order.

3. LEGAL AND CONSTITUTIONAL FRAMEWORK

3.1 Constitutional Foundations of Digital Sovereignty

In the Indian legal order, digital sovereignty rests on the constitutional executive and legislative powers of the Union. Under the Seventh Schedule of the Constitution of India, the Central Government holds exclusive legislative competence over Defence of India (Entry 1), Foreign

Affairs (Entry 10), Atomic Energy and Mineral Resources (Entry 6), and Posts, Telegraphs, Telephones, Wireless, Broadcasting and Other Like Communications (Entry 31).[4] Consequently, cybersecurity policy, offensive cyber capacity, and international digital treaty making fall within the Union's exclusive domain.

Furthermore, Article 51 of the Constitution (Directive Principles of State Policy) obligates the State to promote international peace and security, maintain just and honorable relations between nations, and foster respect for international law and treaty obligations.[5] However, as established in *Jolly George Varghese v Bank of Cochin*[6] and reinforced in *K.S. Puttaswamy v Union of India*,[7] India follows a dualist tradition. International treaties or customary rules governing cyberspace do not automatically become binding internal law under Article 253 unless incorporated by parliamentary statute.

In *Puttaswamy*, the Supreme Court of India recognized the fundamental right to privacy under Article 21 of the Constitution, establishing that state surveillance, data collection, and digital sovereignty assertions must satisfy a three-fold test: (a) explicit legality/statutory authorization, (b) a legitimate state objective (including national security and public order), and (c) strict proportionality.[8] This landmark ruling establishes domestic constitutional bounds on state cyber surveillance and administrative data access during national security crises.

3.2 Statutory Framework: The IT Act 2000 and DPDP Act 2023

India's core legislative instrument for cyberspace is the Information Technology Act 2000 (IT Act), amended substantially in 2008. The IT Act establishes legal mechanisms for cyber infrastructure defense and offense:

- **Section 66F (Cyber Terrorism):** Criminalizes actions committed with intent to threaten the unity, integrity, security, or sovereignty of India, or to strike terror, by denying authorized access to critical computer resources or introducing computer contaminants. It prescribes punishment up to life imprisonment.[9]

- **Section 69 & 69A (Interception and Blocking):** Grants the Central Government broad administrative authority to issue directions for the interception, monitoring, decryption, or public blocking of information through any computer resource in the interest of national sovereignty, state security, friendly relations with foreign states, or public order. [10] The

constitutionality of Section 69A was upheld by the Supreme Court in *Shreya Singhal v Union of India*, provided procedural safeguards under the blocking rules are strictly observed.[11]

• **Section 70 & 70A (Critical Information Infrastructure):** Empowers the government to declare any computer resource essential to national security or economic stability as a Critical Information Infrastructure (CII), establishing the National Critical Information Infrastructure Protection Centre (NCIIPC) as the national nodal agency for its defense.[12]

The legislative framework was augmented by the Digital Personal Data Protection Act 2023 (DPDP Act). While primarily a civilian data protection framework, Section 17 of the DPDP Act provides broad exemptions for government agencies from data processing rules on grounds of state security, public order, and sovereignty.[13] This statutory balance reflects New Delhi's stance that individual privacy rights, while fundamental, remain subject to sovereign national security imperatives in digital space.

4. INTERNATIONAL LEGAL ANALYSIS

4.1 Applicability of Public International Law to Cyberspace

A central debate in international law is whether existing norms derived from physical territorial statehood apply to the virtual, borderless domain of cyberspace. India consistently supports the position reaffirmed in the 2013, 2015, and 2021 UN GGE Reports that established principles of international law, including the UN Charter, apply in full to cyberspace.[14]

International Legal Principle	**Traditional UN Charter / Customary Source**	**Application to Cyber Operations & India's Legal Posture**
Sovereignty (Internal & External)	Customary International Law; ICJ *Nicaragua Case* (1986)	India treats state-owned and private CNI within its territory as protected under sovereign domain. Unauthorized cyber intrusions into CNI constitute a violation of territorial sovereignty per se.
Non-Intervention	UN Charter, Article 2(7); Declaration on Friendly Relations (Res 2625)	Prohibits coercive cyber interference in another state's internal political, economic, or electoral systems (e.g., deepfake election manipulation).

Prohibition on Use of Force	UN Charter, Article 2(4)	Cyber operations causing physical destruction, loss of life, or severe operational disruption to CNI equal a 'use of force' (kinetic equivalence principle).
Inherent Right of Self-Defence	UN Charter, Article 51	Allows defensive counter-cyber or kinetic action if a cyber attack qualifies as an 'armed attack'. India asserts self-defense rights against destructive cyber strikes.
State Responsibility & Due Diligence	ILC Draft Articles on State Responsibility (Articles 4–8)	States must not knowingly allow their digital infrastructure to be used for internationally wrongful acts against third states (due diligence doctrine).

4.2 Sovereignty and the Threshold of 'Use of Force'

Under Article 2(4) of the UN Charter, all members must refrain from the threat or use of force against the territorial integrity or political independence of any state. In physical space, determining a use of force relies on kinetic impact. In cyberspace, where offensive operations typically involve malicious code, malware, or distributed denial-of-service (DDoS) attacks, establishing legal thresholds is complex.

India aligns with the target-based and effect-based approach articulated in the Tallinn Manual 2.0.[15] A cyber operation constitutes a use of force under Article 2(4) if its severity, directness, and measurable consequences are comparable to a traditional kinetic attack such as malware disabling a nuclear facility's cooling system or shutting down an electrical grid during winter. However, for cyber operations falling below the threshold of kinetic force (e.g., espionage, data exfiltration, or defacement), India asserts that such acts remain violations of the principle of non-intervention and sovereign territorial integrity under customary international law.[16]

4.3 The Legal Problem of Attribution and State Responsibility

The primary operational and legal obstacle to cyber-deterrence is **attribution**. Cyber operations frequently utilize proxy threat actors, spoofed IP addresses, compromised foreign servers, and routing networks, concealing the ultimate instigator. Under the International Law Commission's (ILC) Draft Articles on Responsibility of States for Internationally Wrongful Acts, an act is attributable to a state only if conducted by a state organ (Article 4) or by persons

acting under the strict instruction, direction, or control of that state (Article 8).[17]

The ICJ's high evidentiary standard for state control set out in the *Nicaragua Case*[18] and re-affirmed in *Bosnian Genocide*[19] requires proof of "effective control" over specific unauthorized operations. In cyberspace, proving a state exercised effective control over independent hacker collectives or patriotic cyber militias is exceptionally difficult. India argues in multilateral forums like the UN OEWG that international law must evolve to recognize indirect responsibility, holding host states accountable under the **due diligence doctrine** if they knowingly permit proxy actors to operate within their digital borders.[20]

5. FINDINGS: CYBER-DETERRENCE AND AI GOVERNANCE

5.1 India's Evolving Cyber-Deterrence Doctrine

India's strategic posture has shifted from passive defense toward active deterrence. The creation of the Defence Cyber Agency (DCyA) in 2019 marked a structural transition, integrating offensive and defensive cyber capabilities across the Army, Navy, and Air Force.[21]

Analysis reveals that India's cyber-deterrence rests on three operational pillars:

1. **Deterrence by Denial:** Hardening national CNI through NCIIPC, CERT-In, and strict local hosting mandates for military and financial networks. By increasing the technical complexity and financial cost of intrusion, India aims to deter potential adversaries.

2. **Deterrence by Punishment (Active Cyber Defence):** Developing counter-offensive assets capable of penetrating adversary networks to disrupt ongoing hostile cyber operations. Under international law, such active countermeasures are permissible under the ILC Framework (Articles 49–54), provided they are directed solely against the responsible state, are reversible, and conform to strict proportionality.[22]

3. **Multi-Aligned Coalition Building:** Securing bilateral intelligence and cybersecurity cooperation agreements with partners including the Quad (US, Japan, Australia), France, and Israel, alongside active participation in BRICS cybersecurity working groups.

5.2 Artificial Intelligence Governance and Armed Conflict

The integration of Artificial Intelligence into military command-and-control architectures, intelligence processing, and Lethal Autonomous Weapons Systems (LAWS) introduces

pressing international legal questions. Dual-use generative AI models can automate zero-day vulnerability discovery, generate deepfake disinformation campaigns, and accelerate target acquisition cycles.

India's policy on military AI reflects a dual stance: advocating for ethical governance while preserving military modernization requirements:

Compliance with International Humanitarian Law (IHL): India maintains that any deployment of AI in armed conflict must comply with fundamental IHL rules codified in the 1977 Additional Protocol I to the Geneva Conventions specifically *distinction*, *proportionality*, and *precaution in attack*.[23] Autonomous target selection models operating as black-box algorithms often lack explainability, risking misidentification of civilians and protected infrastructure.

Human-in-the-Loop Imperative: In international discussions at the Convention on Certain Conventional Weapons (CCW) in Geneva, India consistently opposes total blanket bans on military AI development, while insisting on the mandatory retention of meaningful human control ("Human-in-the-Loop" or "Human-on-the-Loop") over decisions involving lethal force.[24]

Domestic Regulatory Governance: Domestically, India prioritizes economic growth and ethical guardrails through NITI Aayog's *National Strategy for Artificial Intelligence (#AIforAll)*. However, a dedicated, binding statutory framework governing military AI testing, liability for algorithmic failure, and deployment safety remains under development.

6. SUGGESTIONS

To strengthen India's digital sovereignty, enhance its legal defense posture, and lead global digital governance reform, the following statutory and diplomatic measures are recommended:

1. **Draft and Enact a National Dedicated Cyber Security Act:**

Parliament should enact a comprehensive National Cyber Security Act to update the framework of the IT Act 2000. This legislation should explicitly define critical cyber infrastructure, establish clear legal authority and judicial oversight for offensive counter operations by the Defence Cyber Agency, and mandate standardized breach reporting for both

public and private entities.

2. **Draft an Algorithmic Accountability and Military AI Regulatory Framework:** India should introduce statutory regulations for dual-use and military AI deployments. The law should mandate algorithmic safety audits, require human-in-the loop controls for targeting systems, and establish strict state civil liability standards for algorithmic collateral damage during peacetime security operations.

3. **Institutionalize a Legal Advisory Cell within the Defence Cyber Agency:** Create a dedicated legal Directorate within the DCyA staffed by public international law specialists. This unit would evaluate proposed active cyber countermeasures against international legal standards of necessity, proportionality, and state responsibility prior to execution.

4. **Champion a Global South Coalition on Cyber Attribution Norms:**

India should utilize its diplomatic position within the UN OEWG and BRICS to lead an international effort establishing clear evidentiary standards for cyber attribution. This framework should define when proxy cyber operations trigger state due diligence liabilities, helping prevent arbitrary accusations while holding host states accountable for harboring malicious threat actors.

5. **Secure Bilateral Mutual Legal Assistance Treaty (MLAT) Modernization:** Modernize existing MLAT agreements and sign dedicated cybercrime cooperation treaties with key digital infrastructure jurisdictions. Streamlining cross-border electronic evidence access will enhance India's domestic law enforcement response to foreign cyber threats without compromising international human rights safeguards.

7. CONCLUSION

The concept of state sovereignty has evolved from physical territorial borders into the digital sphere. As cyberspace and artificial intelligence become primary arenas of inter-state friction and hybrid conflict, the Republic of India faces the dual task of protecting its domestic digital ecosystem while shaping international rules for virtual engagement.

India's strategy demonstrates that digital sovereignty requires both domestic technological resilience and international legal engagement. By anchoring its digital policies in constitutional

norms balancing executive national security authorities with fundamental privacy rights India establishes a principled legal approach. Internationally, New Delhi's defense of UN Charter applicability, insistence on meaningful human control over military AI, and rejection of unilateral digital hegemony reflect a balanced multi-alignment stance.

To preserve strategic autonomy in an increasingly volatile digital landscape, India must continue updating its legislative frameworks, establishing clear military cyber operation rules, and advocating for an inclusive international legal order. By pairing operational cyber deterrence capabilities with a commitment to public international law, India can safeguard its sovereign digital future while contributing to global stability in the machine age.

FOOTNOTES

1. Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 11–14.
2. Arindrajit Basu, 'India's Role in Shaping Global Cyber Norms' (2020) 21(2) Melbourne Journal of International Law 312, 315.
3. Ministry of Electronics and Information Technology (MeitY), *India's Trillion-Dollar Digital Economy Report* (Government of India 2019) 45–48.
4. Constitution of India 1950, Seventh Schedule, List I (Union List), Entries 1, 6, 10, 31.
5. ibid art 51(a)–(c).
6. (1980) 2 SCC 360.
7. (2017) 10 SCC 1.
8. ibid [310]–[324] (Chandrachud J).
9. Information Technology Act 2000, s 66F.
10. ibid ss 69, 69A.
11. (2015) 5 SCC 1, [101]–[105].
12. Information Technology Act 2000, ss 70, 70A.
13. Digital Personal Data Protection Act 2023, s 17(1)(a).
14. UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174, paras 24– 28.
15. Schmitt (n 1) 330–337 (Rule 69: Definition of Use of Force).
16. UNGA, 'Official Compendium of Voluntary National Submissions on the

Implementation of International Law in Cyberspace' (13 July 2021) UN Doc A/76/136, Submission of India, 42–46.

17. International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts' (2001) Supplement No 10 (A/56/10) arts 4, 8.
18. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, [115].
19. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Judgment) [2007] ICJ Rep 43, [400].
20. UNGA, 'Statement by India at the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies' (5 March 2024) UN Doc A/RES/75/240.
21. Ministry of Defence, *Annual Report 2019-2020* (Government of India 2020) 38. 22 ILC Draft Articles (n 17) arts 49–53.
22. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 1977, arts 48, 51, 57.
23. UN Office for Disarmament Affairs, 'Statement of the Republic of India to the Group of Governmental Experts on Lethal Autonomous Weapons Systems' (Geneva, 6 March 2023).
24. NITI Aayog, *National Strategy for Artificial Intelligence: #AIforAll* (Government of India 2018)