Digital Sovereignty: The Global South's Predicament and How to Measure It

On 4 September 2025, the Nepalese government made a decision: ban twenty-six international internet platforms from operating in the country, including Facebook, X (formerly Twitter), and YouTube. The government's intent was to control cyberspace. The result was catastrophic. Young people took to the streets — against the ban, but also, as People's Dispatch reported, against the unemployment, corruption, and broken development model behind it. Clashes escalated; more than 70 were killed and over 2,000 injured. Prime Minister K.P. Sharma Oli was forced to resign; the government collapsed. Into the vacuum stepped Balendra Shah — rapper turned politician, leader of the four-year-old Rastriya Swatantra Party (RSP) — who swept the March 2026 elections with a near two-thirds majority. The RSP is part of newly 'engineered forces' that converted Gen Z's digital anger into parliamentary seats. The left parties that had governed Nepal were reduced to single figures. An administrative decision around controlling social media platforms brought down a government. Social media built its replacement.

Nepal's story reveals a fact: digital space has become part of national territory. If a government cannot establish effective sovereignty in digital space, its capacity to govern in the physical world will also disintegrate.

The cloud sounds weightless, dematerialised, floating above the planet. Tricontinental's dossier no. 46, *Big Tech and the Current Challenges Facing the Class Struggle* writes plainly: 'A data "cloud" sounds like an ethereal, magical place. It is, in reality, anything but that.' The cloud is a set of extremely concrete, highly centralised infrastructure: server farms, submarine cables, chip fabrication plants, cooling towers – overwhelmingly located on US soil, subject to US law and US corporate control.

For most countries of the Global South, digital sovereignty remains a distant concept. They have not even begun to examine their own situation.

The Cloud Has a Physical Address

What does the landscape of global digital infrastructure look like?

Ninety per cent of Africa's internet traffic travels through submarine cables owned and operated by European and US companies. The consequences of that dependence became visible in March 2024, when an underwater landslide off the coast of Côte d'Ivoire severed four cables simultaneously. Thirteen African countries along the

western seaboard, including Ghana, Nigeria, and Côte d'Ivoire, lost internet access for weeks. Millions of users were cut off. The outage cost Nigeria alone over $590 million in four days. The companies that own the cables assumed no responsibility for the damage to African economies; repair timelines were determined by the cable owners, not by the countries affected. Afterwards, SpaceX's Starlink rapidly expanded its market share in the region. Once dependency is established, crisis only deepens dependency.

As Bappa Sinha writes in Tricontinental's *Breaking the Stranglehold: How China is Shattering US Technological Hegemony*, for over a century, the foundation of imperial power has been monopolistic control over the most advanced means of production, with military force and financial dominance as supporting instruments. From the industrial revolution through the age of digital platforms, successive imperial cores secured global dominance by capturing technological frontiers, extracting monopoly rents, and reinvesting those rents into further technological leadership, sustaining what appeared to be a self-reproducing hierarchy. The imperial core monopolises technology and capital; the periphery supplies labour and resources; unequal exchange continuously transfers value upward. This structure operates without formal colonial rule. When the Global South passed the New International Economic Order resolution at the United Nations in 1974, demanding technology transfer from North to South as a central provision, the response came two decades later through the Uruguay Round of the GATT: reverse engineering and technology transfer were made illegal. As Vijay Prashad writes in *The Poorer Nations* (Verso, 2012), what replaced the South's demand was not a New International Economic Order but a North-led New International Property Order.

That order now governs the most advanced means of production of our own era: digital infrastructure. Chip manufacturing is concentrated in Taiwan and South Korea (using US-designed architectures). Operating systems are monopolised by Microsoft, Apple, and Google. The cloud computing market is dominated by Amazon AWS, Microsoft Azure, and Google Cloud. The global search engine market belongs almost entirely to Google. Countries, businesses, and citizens of the Global South use this infrastructure every day, but its physical location, jurisdiction, and control rest elsewhere.

Data is at the centre of all this. In April 2020, China's State Council formally designated data as a fifth factor of production — alongside land, labour, capital, and technology. But the economic status of data is deeply ambiguous.

Current international accounting standards do not include data assets on corporate balance sheets. US tech giants, through their global platforms, continuously absorb data generated by users worldwide. No universally accepted method for valuing this data exists; what cannot be measured does not appear on any tax return. Facebook, Google, and Microsoft together avoided $2.8 billion in taxes across twenty developing countries in 2019 alone — a figure researchers describe as 'the tip of the iceberg'. What is not measured is not taxed. What is not taxed is free.

This 'unmeasurability' is itself a mechanism of control. Global South countries cannot even quantify how much value they are losing, let alone assert rights over their data.

Three Structural Challenges, One Structural Trap

The Global South's digital sovereignty predicament can be decomposed into three structural challenges. They reinforce each other and together constitute a structural trap.

1. Severe external dependence on digital infrastructure

From hardware to software to information security, Global South countries rely almost entirely on the US-provided technology stack. Consider Brazil. Its ICT market is $141.7 billion, 6.5 per cent of GDP (per Brasscom, Brazil's ICT industry association), yet only 24.8 per cent of its software is domestically produced, per the *BRICS Digital Sovereignty Index Report* (citing ABES 2024). The cloud computing market is divided among Amazon, Microsoft, and Huawei. When data is stored on foreign companies' servers under foreign legal jurisdiction, 'sovereignty' over that data amounts to a paper claim. South Africa's situation is even more alarming. Scoring low on digital sovereignty assessments, South Africa is not pivoting toward autonomous construction; its EEIP framework, presented as a general policy for multinational ICT firms, would also address one of the principal regulatory obstacles to Starlink's entry into the South African market.

2. Digital governance without sovereignty

Many Global South countries have enacted digital governance legislation, yet these measures have done little to alter the underlying relations of technological dependence. Brazil passed its General Data Protection Law (LGPD) in 2020; India enacted its Digital Personal Data Protection Act in 2023. But the gap between legal text and practical effect is enormous. Brazil's detailed rules on international transfers of personal data only arrived in August 2024, with the ANPD's Resolution CD/ANPD No. 19/2024 — years after the rest of the law took effect. India's data protection law allows data to flow freely to any country except those on a government 'blacklist'. Given US tech companies' total penetration of India's digital economy, this is an open door.

A 2020 World Economic Forum white paper went so far as to argue that governments only need 'remote access' to data held by companies; where the data is stored does not matter. The substance of this proposal is to maintain the status quo, ensuring Global South countries continue to hand all their data to US tech giants. Passivity in governance rules stems from asymmetry of power. When your infrastructure depends on others, your authority to make rules is limited.

3. Systematic erosion of domestic digital capabilities

This may be the most fundamental challenge. Brazil once pursued an ambitious strategy to build a domestic computing industry. Its 1984 Informatics Law reserved much of the domestic market for Brazilian firms, covering computer hardware, software, databases, and other digital products. By the late 1980s, this strategy had helped create a sizeable domestic computer sector. But under the Collor government in the early 1990s, trade liberalisation and the dismantling of market-reserve policies exposed local firms to foreign competition before they had reached technological maturity. Brazil was thus integrated into the global digital economy increasingly as a market for imported technologies rather than as a producer of them.

India followed a different path but reached a similar outcome. Semiconductor Complex Limited, approved in 1976 and producing chips by 1984, represented an early attempt to build indigenous semiconductor capacity. A major fire in 1989 destroyed much of the Mohali facility and set back the project, but the deeper problem was the absence of sustained state investment and industrial strategy after that rupture. As Taiwan, South Korea, and later China invested heavily in semiconductor fabrication, India's economic reforms increasingly prioritised software and IT services over manufacturing. The consequences remain visible today: while China's leading foundries are producing chips at 3-nanometre and below, India's domestic fabrication capability remains concentrated in legacy process nodes, while advanced chips continue to be manufactured abroad. India became a global centre for software labour while remaining dependent on foreign firms for advanced semiconductor manufacturing.

In both cases, integration into global value chains occurred through subordinate positions: Brazil as a market for foreign digital products, India as a supplier of software services without control over the hardware base. The result was not simply technological backwardness, but the erosion of complete national digital ecosystems.

Industrial hollowing-out leads to brain drain, brain drain leads to declining policy judgment, declining judgment allows Western consulting firms to easily dominate the policy agenda. But what is most worrying is the shift in industrial elites' own thinking. Nandan Nilekani, Chairperson of Infosys (one of India's largest IT services firms), stated publicly at Meta's 'Build with AI' summit in Bengaluru in 2024: 'Our goal should not be to build one more LLM [large language model]. Let the big boys in Silicon Valley do it, spending billions of dollars. We will use it…' The CEO of Tata Consultancy Services (TCS), India's largest IT services company, said something similar. When the leaders of a country's largest IT companies consider fundamental R&D to be someone else's business, digital sovereignty is out of the question.

The three challenges reinforce each other. Infrastructure dependence weakens the material basis for autonomous governance. Passive acceptance of governance rules compresses the space for industrial policy. Digital capability gaps fundamentally undermine the capacity to recognise and address the first two problems. Together they constitute a structural trap.

You Cannot Change What You Cannot Measure

Digital sovereignty varies enormously among Global South countries, and a blanket 'South versus North' narrative cannot capture this variation. To formulate effective policy, a measurement tool is needed, one that can systematically diagnose each country's digital sovereignty condition.

The Digital Sovereignty Index (DSI) is such a tool. Developed in 2025 by Xiong Jie — senior researcher at Tricontinental and Secretary-General of the Global South Academic Forum — the DSI decomposes digital sovereignty into four dimensions and sixteen specific indicators, each evaluated on a five-level maturity scale.

Data ownership autonomy is the concentrated expression of digital sovereignty. Without ownership of data, nothing else is possible. This dimension includes four indicators: data ownership legislation (whether the state has established a clear legal framework for data property rights), domestic data storage requirements (whether

critical data must be stored within national borders), cross-border data flow protection (whether adequate safeguards exist when data leaves the country), and data value public benefit inclusion (whether value generated by user data flows to the public rather than being extracted as private profit by foreign platforms).

But data ownership cannot be realised in a vacuum. It requires the support of **digital infrastructure autonomy**. This dimension examines the degree of independence across four layers: basic hardware (chips, servers, storage devices), basic software (operating systems, databases, middleware, cloud platforms), application software, and information security.

Digital space governance autonomy ensures that a country can shape, not merely accept, the rules of digital space. Those rules are currently written through a set of bodies where the US holds structural influence: the Internet Corporation for Assigned Names and Numbers (ICANN) over domain names and internet addressing, the Internet Engineering Task Force (IETF) over core protocols, the Institute of Electrical and Electronics Engineers (IEEE) over technical standards, and the World Trade Organization's Agreement on Trade-Related Intellectual Property Rights (TRIPS) over intellectual property — the same framework Prashad names as the 'New International Property Order'. This dimension measures a country's capacity to legislate domestically *and* to contest those international arenas rather than inherit their outcomes.

All three dimensions above depend on **digital capability autonomy**. This dimension assesses cutting-edge technology R&D, university STEM talent cultivation, industrial engineering capacity, and the degree of coordination between digital technology and national development strategy.

A clear logical relationship exists among the four dimensions. Data ownership autonomy is the concentrated manifestation of digital sovereignty, but its realisation requires infrastructure autonomy as a material foundation and governance autonomy as an institutional guarantee. All three depend on digital capability autonomy as the fundamental support. The structure of the DSI framework itself reveals the operating mechanism of the structural trap: if digital capability is insufficient, infrastructure and governance cannot be autonomous; if infrastructure is not autonomous, data ownership can only be a paper claim.

Each indicator uses a five-level maturity scale: Level 1 'Initial' (the issue of autonomy in this area has not been recognised); Level 2 'Aware' (the importance has been recognised, initial actions are being taken); Level 3 'Developing' (active progress is underway, but significant dependence remains); Level 4 'Competent' (strong international competitiveness); Level 5 'Independent' (largely autonomous, with little constraint from other countries).

In March 2026, the International Communication Research Institute at East China Normal University, the Global South Academic Forum, and the Institute for Digital Economy & Artificial Systems (IDEAS) officially released the *BRICS Digital Sovereignty Index Report* at the Zhongguancun Forum. The findings are striking: China leads across all four DSI dimensions; Russia and India show strength in specific areas. But most of the newly admitted BRICS member countries — drawn from the broader Global South — remain at the earliest stages on infrastructure and core technologies. The structural trap described above is not an abstraction. It is what the numbers show.

The Same Label, Different Realities

The *BRICS Digital Sovereignty Index Report's* assessment results reveal a critical fact: beneath the uniform label of 'Global South', countries' digital sovereignty conditions differ dramatically.

China (DSI average 4.25) is the only country besides the United States with relatively complete digital sovereignty. Most indicators reach 'Competent' or 'Independent' levels. China's relative weakness lies in international digital space rule-making, though its influence in international standards organisations has been growing steadily.

Russia (3.25) presents a distinctive case. Western geopolitical pressure and sanctions have pushed Russia to pursue digital sovereignty more aggressively. Russia scores highly on application software (5/Independent), basic software (4/Competent), information security (4), and talent cultivation (4). But it faces a severe bottleneck: chips. Basic hardware autonomy scores only 3 (Developing), with heavy reliance on imports. In 2021, Russia held just 1,973 international patents, 0.35 per cent of the global total. This figure dropped sharply in 2022–23 under Western restrictions.

India (2.94) is a classic case of one strong leg. The digital capability dimension is its bright spot: 2.55 million STEM graduates in 2020, second globally behind China, with a massive IT services ecosystem. But India is severely lopsided: focused on the application layer, doing almost no fundamental R&D. Core hardware and basic software depend heavily on US supply. Data protection legislation was only recently enacted and remains untested. Government investment is limited; brain drain is severe.

Brazil (2.13) appears fragile across all dimensions. After abandoning its domestic ICT industry, both the industrial base and talent pool are thin. Building independent digital infrastructure in the short term would be extremely difficult. The DSI report states bluntly: Brazil's digital sovereignty remains fragile, highly dependent on Western companies.

South Africa (1.94) has relatively complete data protection legislation and a clear digital strategy on paper, but the gap between paper and reality is vast: weak enforcement, deep dependence on foreign core infrastructure, and domestic R&D constrained by limited resources and brain drain. Policy intent and legal frameworks fall far short of achieving digital sovereignty. Rather than pivoting toward autonomous construction, South Africa's policy framework would ease Starlink's entry into its market — suggesting that the political will to pursue digital sovereignty is itself weak.

Placed side by side, several judgments emerge. China is the exception; the rule is that most Global South countries' digital sovereignty falls far below what outsiders might imagine. Patent data is especially stark: the US holds 21.11 per cent of global patents, China 39.84 per cent, Russia 0.35 per cent, Brazil 0.04 per cent, South Africa 0.01 per cent. The STEM graduate gap is equally telling: China 3.57 million, India 2.55 million, US 820,000, Russia 520,000, Brazil 238,000. The DSI assessment quantifies a reality that has long been treated with vagueness, forcing into view what the dominant powers have preferred to leave unmeasured: the full depth of the Global South's digital dispossession.

The Window Is Closing

The DSI assessment does more than diagnose the present; it points toward a grim prospect. For most Global South countries, the historical window for independently building a complete ICT industry is narrowing. The capital threshold for the ICT industry is extreme. China and the United States each invest hundreds of billions of dollars annually in AI R&D. India's national AI programme (IndiaAI) has a budget of $1.25 billion. The gap is two orders of magnitude.

But a narrowing window does not mean no options exist. Sinha notes that China's development strategy centres on production, not rent extraction. Through long planning horizons, state coordination, mass technical education, and disciplined capital allocation, China has systematically built complete industrial ecosystems across multiple advanced sectors simultaneously. The socialist state has prevented domestic capital from consolidating into monopoly forms capable of extracting sustained super-profits. Firms are compelled to compete on cost, quality, and process innovation rather than relying on intellectual property rents. As a result, China has repeatedly transformed technologies that the imperial core treated as rent-generating monopolies into competitive, low-cost commodities.

This means Global South countries face a choice between two different logics. The US system operates on technological monopoly and rent extraction, using intellectual property regimes, trade agreements, and 'multi-stakeholder' governance frameworks to lock the Global South into permanent payment and permanent dependence. The alternative — demonstrated by China's own development path — is production diffusion and technological democratisation: compressing monopoly rents into competitive costs, transferring capabilities rather than licensing access to them, building industrial ecosystems through state coordination rather than market extraction. South-South cooperation organised around this logic is not another form of dependency; it is the only credible path through a closing window.

The value of the DSI lies in enabling Global South countries to see their own full picture: which dimensions have foundations, which are weak points, where cooperation space exists, which links must remain under autonomous control. Measurement is the precondition for action. With diagnosis comes the possibility of strategy.