Delhi Policy Group

Advancing India's Rise as a Leading Power

POLICY BRIEF

Rethinking Power in the Digital Age

Authors

Deependra Singh Hooda

Pavithran Rajan

Volume X, Issue 26

October 9, 2025

Delhi Policy Group

Core 5A, 1st Floor, India Habitat Centre, Lodhi Road, New Delhi- 110003

www.delhipolicygroup.org

Delhi Policy Group
Advancing India's Rise as a Leading Power

Policy Brief Vol. X, Issue 26
October 9, 2025

ABOUT US

Founded in 1994, the Delhi Policy Group (DPG) is among India's oldest think tanks with its primary focus on strategic and international issues of critical national interest. DPG is a non-partisan institution and is independently funded by a non-profit Trust. Over past decades, DPG has established itself in both domestic and international circles and is widely recognised today among the top security think tanks of India and of Asia's major powers.

Since 2016, in keeping with India's increasing global profile, DPG has expanded its focus areas to include India's regional and global role and its policies in the Indo-Pacific. In a realist environment, DPG remains mindful of the need to align India's ambitions with matching strategies and capabilities, from diplomatic initiatives to security policy and military modernisation.

At a time of disruptive change in the global order, DPG aims to deliver research based, relevant, reliable and realist policy perspectives to an actively engaged public, both at home and abroad. DPG is deeply committed to the growth of India's national power and purpose, the security and prosperity of the people of India and India's contributions to the global public good. We remain firmly anchored within these foundational principles which have defined DPG since its inception.

Authors

Lt. Gen. Deependra Singh Hooda (Retd.), PVSM, UYSM, AVSM, VSM & Bar, Distinguished Fellow for Military Strategy, Delhi Policy Group
Lt. Col. Pavithran Rajan (Retd.)

The views expressed in this publication are those of the authors and should not be attributed to the Delhi Policy Group as an Institution.

Cover Image:

US President Donald Trump and First Lady Melania Trump hosted tech leaders for a dinner in the State Dining Room of the White House in Washington, DC, on September 4, 2025. Source: White House

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre,
Lodhi Road, New Delhi- 110003
www.delhipolicygroup.org

Rethinking Power in the Digital Age

by

Deependra Singh Hooda and Pavithran Rajan

Contents

Rethinking Power in the Digital Age

by

Deependra Singh Hooda and Pavithran Rajan

The New Architecture of Power

In May 2019, the United States added Huawei to its "Entity List", effectively cutting off the Chinese telecommunications giant from accessing Google's Android services and advanced semiconductors. From being the number one smartphone brand globally in mid-2020, Huawei's market share worldwide dropped from 15% in 2020 to just 3% in 2021.[1] This massive loss in sales effectively ended Huawei's global ambitions in the smartphone market.

Further restrictions followed on China, most notably the Dutch decision (under US pressure) to block exports of ASML's most advanced Extreme Ultraviolet (EUV) lithography tools. Currently, China lacks the capability to replicate ASML's lithography technology, which has placed significant constraints on its ability to produce advanced chips.[2]

These examples illustrate a fundamental shift in how power operates in the 21st century. When we consider national power, we naturally focus on traditional instruments, such as the size of militaries, diplomatic heft, or economic muscle, in shaping global influence. However, this conventional view increasingly misses the most consequential power struggle of our times.

The real contest for influence today is being fought in the arena of the technological substrate. This brief introduces the concept of the substrate, which encompasses both the physical hardware (fabs, chips, internet cables, data centres, etc.) and the invisible layers (routing protocols, operating systems, social media algorithms, technical standards, etc.) that keep modern societies running.

Export controls on technology can significantly impact a state's military, economic, and technological capabilities. Protocols, programming interfaces, and algorithms determine who can gain access, on what terms, and the level of visibility of a narrative. Control over where data resides and how it moves enables surveillance, intelligence

[1] Friedman, Alan. "U.S. Bans Lead to a Decline of over 81% in Huawei's Phone Shipments during 2021." PhoneArena, January 30, 2022. https://www.phonearena.com/news/smartphone-shipments-by-huawei-decline-sharply-in-2021_id138129.
[2] Shivakumar, Sujai, Charles Wessner, and Thomas Howell. Balancing the Ledger: Export Controls on U.S. Chip Technology to China. February 21, 2024. https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china.

gathering, and jurisdictional authority. The substrate is therefore the arena which is increasingly coming to define power.

Existing international relations theories do not adequately explain contemporary power dynamics. Classical realism assumes sovereignty as a formal attribute of statehood and suggests that power is contingent upon military capability, economic strength, and geographical control. However, this framework does not adequately address the vulnerabilities created by dependencies on foreign-owned technologies.

Liberalism's faith in international institutions and economic interdependence offers little relief when actors that control the infrastructure, such as SWIFT messaging or cloud providers, can simply switch others off.[3] Even constructivist approaches, which focus on beliefs, identity, norms, and social interaction, overlook the crucial role of technological architecture, which can constrain choices.

The dynamics of the substrate become most apparent when examining the experiences of developing nations. Despite being independent, many countries find themselves locked into technological dependencies that limit their policy options and narrow the scope for independent decision-making.

The concept of a "substrate" builds upon prior scholarship, such as Martin C. Libicki's work, which treats cyberspace as a layered system. However, while Libicki focuses on military and cybersecurity implications, our framework expands the substrate to include domains that address broader geopolitical dynamics and outcomes related to sovereignty.

The Substrate Framework

Understanding the substrate begins with a simple recognition: in the digital age, power flows through both physical and invisible technological infrastructure. This substrate operates across four interconnected domains, each representing a crucial dimension of technological power.

The first domain is computational infrastructure - the hardware and systems that store and process data and enable digital services. This includes components like data centres, cloud platforms, and the entire semiconductor supply chain, from raw materials to advanced chip fabrication.

[3] Analytics, F. P. "What Does Russia's Removal From SWIFT Mean For the Future of Global Commerce?" Foreign Policy, October 2, 2022. https://foreignpolicy.com/2022/03/08/swift-sanctions-ukraine-russia-nato-putin-war-global-finance/.

A few players dominate the cutting-edge technologies of this infrastructure. Taiwan Semiconductor Manufacturing Company manufactures over 68% of the world's semiconductors, accounting for more than 90% of the most advanced chips (those using 5nm, 3nm, and smaller process nodes).[4] ASML controls over 90% of the global market for lithography tools, and it is the sole supplier of EUV systems, which are critical for producing the most advanced semiconductors.[5] American companies, including Amazon, Microsoft, and Google, collectively control approximately 65% of the global cloud infrastructure market share.[6] Nvidia controls between 70% and 95% of the market for AI chips used for training and deploying models, such as OpenAI's GPT.[7]

This concentration creates extreme leverage for those who control these vital resources and vulnerability for those who depend on them.

The second domain encompasses network architecture - the physical and logical systems that enable communication and data flow. Undersea cables, which carry over 95% of intercontinental internet traffic, are owned and operated by a relatively small number of private companies and state-owned enterprises. American engineers primarily designed the routing protocols that determine how data moves across the internet. Although internet governance has broadened, concerns persist about trust, equity, and access.

This domain includes the interoperability protocols that reside in firmware, routers, base stations, and servers. States dependent on foreign-controlled networks are vulnerable to surveillance, disruption, or disconnection. When China pushes for a new internet protocol or Russia creates a 'sovereign internet', they are not merely pursuing technological innovation but attempting to reduce dependence on US-dominated protocols.[8]

The third domain is the information systems, the databases, algorithms, and platforms that organise and process the world's data. This includes everything from the GPS

[4] "Taiwan Makes the Majority of the World's Computer Chips. Now It's Running Out of Electricity | WIRED." Accessed September 28, 2025. https://www.wired.com/story/taiwan-makes-the-majority-of-the-worlds-computer-chips-now-its-running-out-of-electricity/.
[5] "ASML: The EUV Lithography Giant Navigating Challenges." Accessed October 7, 2025. https://finance.yahoo.com/news/asml-euv-lithography-giant-navigating-130136031.html?guccounter=1.
[6] "The Latest Cloud Computing Statistics (Updated January 2025) | AAG IT Support." Accessed September 28, 2025. https://aag-it.com/the-latest-cloud-computing-statistics/.
[7] Leswing, Kif. "Nvidia Dominates the AI Chip Market, but There's More Competition than Ever." CNBC, June 2, 2024. https://www.cnbc.com/2024/06/02/nvidia-dominates-the-ai-chip-market-but-theres-rising-competition-.html.
[8] Yin, Jessie. "The Race for Cyberspace: China's IP Standards and the Threat to Net Neutrality." Articles. Chinaobservers, October 10, 2024. https://chinaobservers.eu/the-race-for-cyberspace-chinas-ip-standards-and-the-threat-to-net-neutrality/.

satellites that enable navigation to the social media platforms that shape public discourse and sentiment. A handful of American and Chinese companies control the platform economy through which billions of people access information, services, and conduct commerce.[9]

Control over these systems provides deep insight into human behaviour and enormous influence over information flows. These platforms do not merely reflect existing power structures, but actively shape them through algorithmic design, content moderation policies, and governance decisions.

The fourth domain encompasses regulatory controls, standards bodies, and certification processes that provide powerful tools for controlling technological development and deployment. Standards bodies play a critical role in shaping key aspects of technology, from wireless communication protocols to internet governance. Participation in these bodies requires significant technical expertise and sustained engagement, advantages that tend to favour established powers. The standards that emerge from these processes determine technological development worldwide. States absent from standards-setting and regulatory arenas risk having their technological environments shaped by the preferences of others.

China's rise in 5G technology demonstrates how strategic engagement with standards bodies can reshape global tech systems. While Western companies treated the 3rd Generation Partnership Project (3GPP) as a technical forum, China recognised it as a strategic space. Starting in the early 2010s, Chinese companies like Huawei, ZTE, and China Mobile deployed large teams to 3GPP meetings. They systematically contributed thousands of technical proposals, built extensive patent portfolios, and secured leadership roles in key working groups. When 5G standards were finalised, Chinese companies held significant portions of essential patents and had embedded their preferred technical approaches into the global standard.[10] As countries deployed 5G networks, Chinese equipment became not just competitive but often necessary to implement the standard that Chinese firms had helped design.

This substrate view of power helps explain some of the contemporary trends in state behaviour. Why does the US invest so heavily in controlling internet routing and restricting access to advanced semiconductors? Why has China committed enormous resources to developing indigenous capabilities in chipmaking, telecommunications equipment, and AI? Why do European leaders speak increasingly about "digital

[9] "15 Facts About The Platform Economy Growth In 2024 & 2025." November 1, 2024. https://marketplacer.com/blog/15-facts-you-should-know-about-the-platform-economy/.
[10] Light Reading. "Study: Huawei Was the Biggest Contributor to 5G Standards." Accessed September 28, 2025. https://www.lightreading.com/5g/study-huawei-was-the-biggest-contributor-to-5g-standards.

sovereignty" and "strategic autonomy"? Why are Nvidia AI chips and the TikTok algorithm so central in the US-China trade talks? The answer is that these actors explicitly recognise that the substrate has become a key element of power. Traditional metrics, such as military spending, GDP, and territorial size, remain important, but equally important is control over the substrate.

A militarily powerful nation can be constrained by its dependence on foreign-controlled supply chains. A 2022 US Department of Defense Report "Securing Defense-Critical Supply Chains" states "The migration of semiconductor manufacturing to the Asia-Pacific region, and the subsequent decline in domestic manufacturing, represents a substantive security and economic threat for the United States."[11]

Even nations with strong institutions and democratic governance can find their policy choices constrained by technological dependencies. Smaller countries are increasingly forced to choose between competing technological systems controlled by different major powers. The case of Huawei's 5G network is illustrative, with the US pressuring nations to ban Huawei, and the Chinese company providing attractive pricing that many countries have found irresistible. These choices have consequences that extend beyond the immediate technical decision, as they shape issues from economic opportunities to security vulnerabilities to cultural influences.

The New Geography of Control

Recognising technological infrastructure as the new arena of power competition requires us to map the world differently. Instead of focusing only on territorial boundaries, we must understand the data flows, the location of critical facilities, and the relationship of technological dependency. This new geography reveals unexpected vulnerabilities and asymmetries.

Singapore's strategic location made it a trading hub in the age of maritime commerce. Today, its dense cluster of submarine cables and hyperscale data centres makes it even more critical in the digital age. Ireland's favourable tax policies attracted American technology companies, but the resulting concentration of European data processing creates strategic exposure.

The map of technological control often diverges sharply from the map of political authority. Critical infrastructure may be physically located in one country while owned and operated by entities based in another. Data about European citizens flows

[11] Securing Defense-Critical Supply Chains. https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF

through servers controlled by Americans. Chinese-manufactured equipment carries internet traffic across Africa and Latin America. American social media platforms have a significant influence on global political discourse.

These alignments create new forms of extraterritorial power projection. When the US imposes sanctions on the use of American technology, it effectively extends its regulatory authority worldwide. When China requires data localisation for its domestic market, it influences the global data flows. When European regulators impose privacy requirements, they compel platforms worldwide to redesign their systems to stay compliant.

The Sovereignty Trap

Understanding the substrate is particularly crucial for developing nations, which often find themselves caught between competing technological powers while lacking the resources to build indigenous alternatives. Traditional development models assumed that countries could adopt foreign technologies and gradually develop their capabilities over time. This approach worked reasonably well in the past, when technologies were often more modular and the pace of change was slower. A country could license manufacturing technology, reverse-engineer products, and develop competitive alternatives.

However, digital technologies often exhibit a winner-takes-all dynamic, making the traditional catch-up model much more difficult. When everyone uses the same social media platform, messaging service, or payment system, the value of alternatives diminishes rapidly. If software ecosystems become entrenched, switching costs can become prohibitive. When data advantages compound over time, early leaders can become nearly impossible to challenge. This is the playbook by which Apple, Google, and Meta have maintained their monopolies.

This creates what could be called the "technological sovereignty trap". Developing nations require access to advanced technologies to foster economic growth and effectively serve their people. However, this access often comes with dependencies that compromise their strategic autonomy. Accepting Chinese telecommunications infrastructure may provide immediate benefits, but it creates long-term vulnerabilities. Relying on American cloud services may enable rapid digital transformation, but it weakens national regulatory control. A country that builds its digital infrastructure around foreign platforms may find it extremely difficult to switch to domestic alternatives later.

Understanding power through the lens of the substrate reveals that dependence is embedded in the very architecture of digital connectivity. For nations seeking digital sovereignty, the challenge is not to completely eliminate these dependencies but to recognise and manage them.

Reclaiming Strategic Autonomy

For middle powers such as India that aspire for strategic autonomy in the digital age, the goal is to reduce structural dependencies over time while remaining integrated within global networks. The following policy imperatives outline the pathway to achieve this.

First, countries must develop sophisticated maps of their technological dependencies. Most nations have detailed intelligence about military threats and economic vulnerabilities, but few nations comprehensively understand their technological vulnerabilities. This mapping exercise should extend beyond obvious domains, such as telecommunications and semiconductors, to include less visible but equally critical areas, such as software dependencies, data flows, and standards compliance.

Second, nations must make strategic investments in critical technological capabilities. This does not mean achieving self-sufficiency across the entire substrate, an impossible task for all but the largest powers. Instead, it means identifying the most strategically essential capabilities and developing indigenous alternatives, as well as resilient and diversified supply chains.

Third, countries should actively participate in the governance of technological standards and protocols. Much of the global technological infrastructure reflects the interests of the actors who shaped its initial development. Nations that wish to influence future technological evolution must engage actively in standards bodies, open-source projects, and international forums governing digital norms.

Fourth, developing nations should explore opportunities for technological cooperation that reduce dependence on major powers. Regional initiatives, such as Africa's Digital Single Market and the EU's Indo-Pacific Digital Partnership, provide models for countries to pool resources and develop shared technological capabilities.

Fifth, all nations must invest in technological literacy among their policy-making elite. The complexity of modern technological systems means that people who do not fully understand their implications often make crucial decisions. This creates opportunities for more technologically sophisticated actors to embed their interests, which might appear neutral but lean towards particular outcomes.

Sixth, nations must build legal and policy frameworks that reduce their exposure to foreign control. This includes preparing for situations where other countries might restrict access to critical technologies through export controls or data policies. Countries like India, with a large and growing digital market, can leverage legal frameworks to shape how global technology firms operate within their borders.

Conclusion

Understanding the substrate is about recognising that the most important battles of the 21st century will be fought over questions that most people rarely consider: Who controls the chips? Who sets the standards? Who owns the data? Who writes the code? These may seem like technical questions, but they are fundamentally political ones. The architecture of the current technological systems defines power and the meaning of sovereignty.

Nations that fail to understand these dynamics will find themselves increasingly locked into the sovereignty trap, where short-term gains from adopting foreign technologies harden into long-term dependencies that erode autonomy. Conversely, those that map their dependencies, invest in critical capabilities, engage in standards bodies, and build coalitions can carve out space for strategic autonomy, even if they cannot master the entire substrate.

***

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre, Lodhi Road
New Delhi - 110003
India

www.delhipolicygroup.org