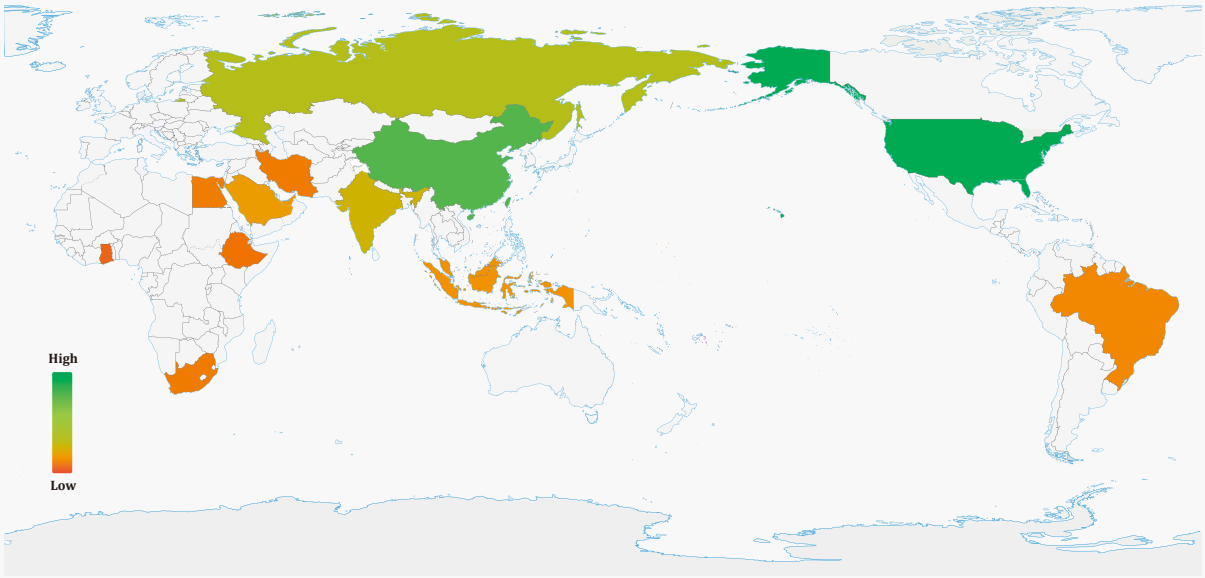
全球南方学术论坛
GLOBAL SOUTH ACADEMIC FORUM

BRICS Partnership on New Industrial Revolution BPI
IDEAS
Institute for Digital Economy & Artificial Systems

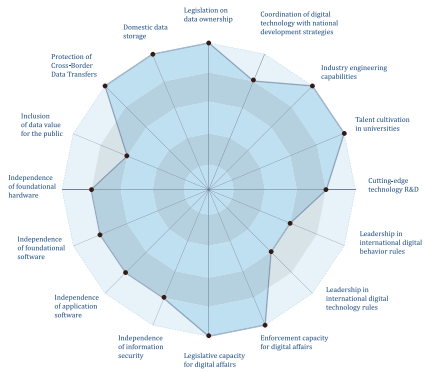
BRICS Digital Sovereignty Index Report

March 2026

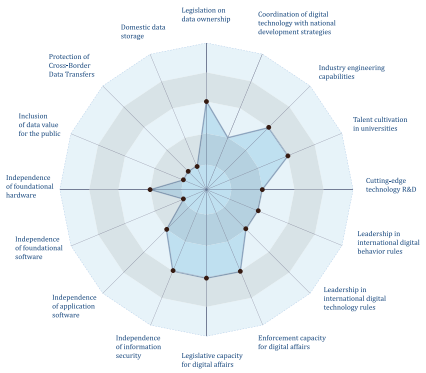
Overview of Digital Sovereignty Index by Country



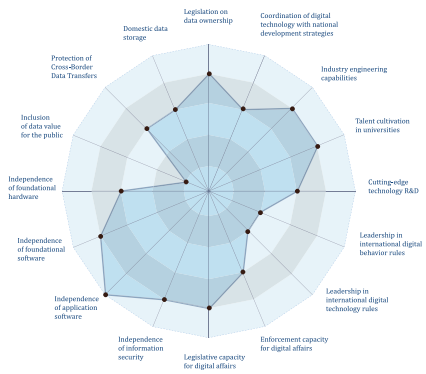
China's Digital Sovereignty Index Assessment Results



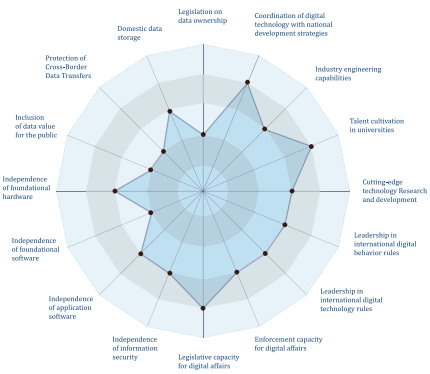
Brazil's Digital Sovereignty Index Assessment Results



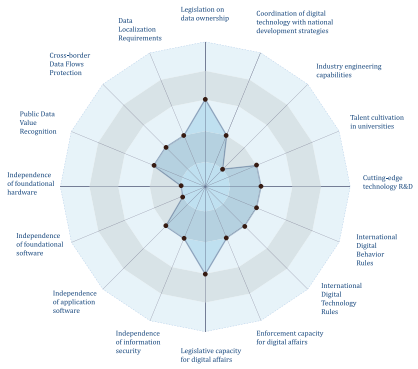
Russia's Digital Sovereignty Index Assessment Results



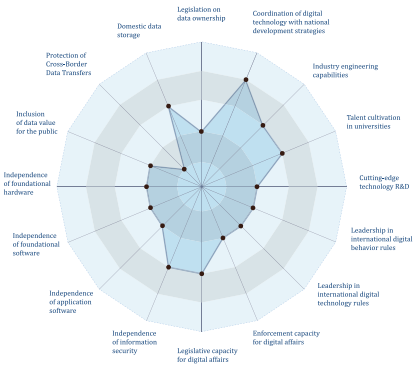
India's Digital Sovereignty Index Assessment Result



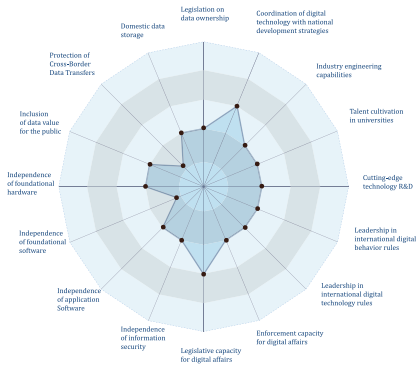
South Africa Digital Sovereignty Index Assessment Results



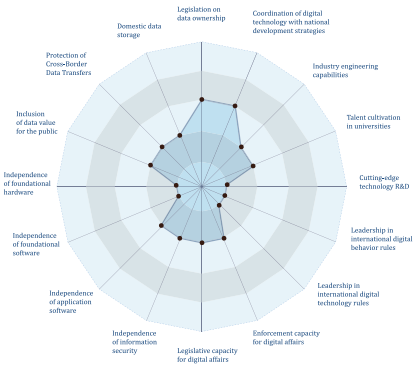
UAE Digital Sovereignty Index Assessment Results



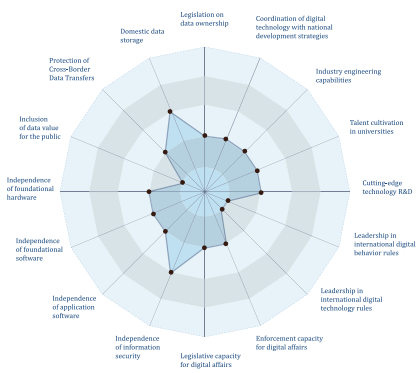
Egypt Digital Sovereignty Index Assessment Results



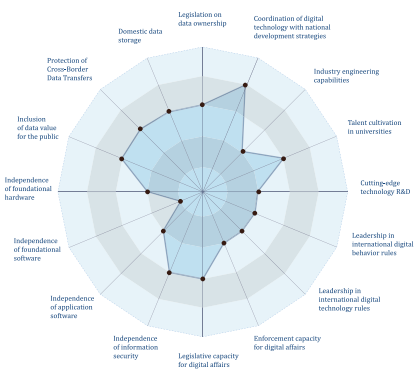
Ethiopia Digital Sovereignty Index Assessment Result



Iran Digital Sovereignty Index Assessment Results



Saudi Arabia Digital Sovereignty Index Assessment Results



Indonesia Digital Sovereignty Index Assessment Results

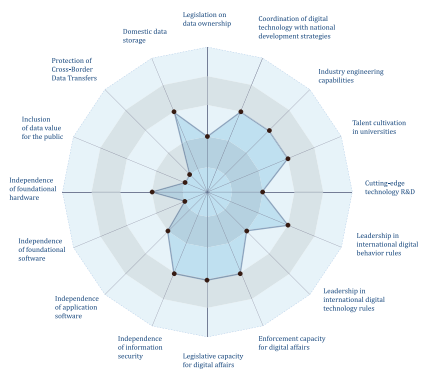


TABLE OF CONTNETS

About This Assessment 6

Digital Sovereignty from a Global South Perspective: National Attitudes and Measurement Systems 9

I. The Rise of the Concept of Digital Sovereignty 10
II. Different Approaches to Digital Sovereignty Among Countries Under the North-South Pattern 12
III. Two Existing Measurement Systems for Digital Space Independence and Their Limitations 16
IV. The Necessity and Possibility of a "Digital Sovereignty Index" Based on the Principle of Independence and Autonomy 17
V. DSI Assessment Methodology and Examples 19
Summary and Outlook 21

China Digital Sovereignty Index Assessment Report 25

China's Data Ownership Independence Status 26
China's Digital Infrastructure Independence Status 29
China's Digital Governance Independence Status 34
China's Digital Capability Independence Status 37
Conclusion and Outlook 40

Brazil's Digital Sovereignty Index Assessment Report 41

Current State of Brazil's Data Ownership Independence 42
Current State of Brazil's Digital Infrastructure Independence 44
Current State of Brazil's Digital Governance Independence 47
Current State of Brazil's Digital Capability Independence 50
Conclusions and Outlook 52

Russia Digital Sovereignty Index Assessment Report 53

Russia Data Ownership Independence Status 54
Russia Digital Infrastructure Independence Status 56
Russia Digital Governance Independence Status 61
Russia Digital Capability Independence Status 63
Conclusion and Outlook 65

India Digital Sovereignty Index Assessment 67

Overview 67
Dimension 1: Data Ownership Independence (2.25/5.0) 68
Dimension 2: Digital Infrastructure Independence (2.75/5.0) 69
Dimension 3: Digital Governance Independence (3.5/5.0) 70
Dimension 4: Digital Capability Independence (3.25/5.0) 71
Summary 72

South Africa Digital Sovereignty Index Assessment 73

Overview 1
Dimension 1: Data Ownership Independence (2.25/5.0) 74
Dimension 2: Digital Infrastructure Independence (1.50/5.0) 74
Dimension 3: Digital Governance Independence (2.25/5.0) 75
Dimension 4: Digital Capability Independence (1.75/5.0) 76
Summary 77

United Arab Emirates Digital Sovereignty Index Assessment 79

Overview 79
Dimension 1: Data Ownership Independence (2.00/5.0) 80
Dimension 2: Digital Infrastructure Independence (2.25/5.0) 80
Dimension 3: Digital Governance Independence (2.25/5.0) 81
Dimension 4: Digital Capability Independence (3.00/5.0) 82
Summary 83

Egypt Digital Sovereignty Index Assessment ····· *85*

Overview ····· *85*
Dimension 1: Data Ownership Independence (1.75/5.0) ····· *86*
Dimension 2: Digital Infrastructure Independence (1.75/5.0) ····· *86*
Dimension 3: Digital Governance Independence (2.25/5.0) ····· *87*
Dimension 4: Digital Capability Independence (2.25/5.0) ····· *88*
Summary ····· *89*

Ethiopia Digital Sovereignty Index Assessment ····· *91*

Overview ····· *91*
Dimension 1: Data Ownership Independence (2.25/5.0) ····· *92*
Dimension 2: Digital Infrastructure Independence (1.50/5.0) ····· *92*
Dimension 3: Digital Governance Independence (1.50/5.0) ····· *93*
Dimension 4: Digital Capability Independence (2.00/5.0) ····· *94*
Summary ····· *95*

Iran Digital Sovereignty Index Assessment ····· *97*

Overview ····· *97*
Dimension 1: Data Ownership Independence (2.00/5.0) ····· *98*
Dimension 2: Digital Infrastructure Independence (2.25/5.0) ····· *98*
Dimension 3: Digital Governance Independence (1.50/5.0) ····· *99*
Dimension 4: Digital Capability Independence (2.00/5.0) ····· *100*
Summary ····· *100*

Saudi Arabia Digital Sovereignty Index Assessment ····· *103*

Overview ····· *103*
Dimension 1: Data Ownership Independence (3.0/5.0) ····· *104*
Dimension 2: Digital Infrastructure Independence (2.0/5.0) ····· *104*
Dimension 3: Digital Governance Independence (2.25/5.0) ····· *105*
Dimension 4: Digital Capability Independence (2.75/5.0) ····· *105*
Summary ····· *106*

Indonesia Digital Sovereignty Index Assessment ····· *107*

Overview ····· *107*
Dimension 1: Data Ownership Independence (2.75/5.0) ····· *108*
Dimension 2: Digital Infrastructure Independence (2.75/5.0) ····· *108*
Dimension 3: Digital Governance Independence (2.75/5.0) ····· *109*
Dimension 4: Digital Capability Independence (2.75/5.0) ····· *110*
Summary ····· *111*

Beyond the Multitude: State–Society Alliances as a Strategy Against Big Tech's Digital Hegemony ····· *113*

The Problem's Roots: The Negrian Framework and Digital Hegemony Critiques ····· *114*
Consciousness of Contradiction: Comprehending Digital Hegemony Through Multiple Contradictions ····· *116*
Struggle Strategy: The Ineffectiveness of the Spontaneous Struggles of the Multitude ····· *118*
Organisational Method: The Dead End of Technology-Based Direct Democracy Attempts ····· *119*
State Participation: Rejecting State Involvement in Building Digital Space ····· *122*
Conclusion ····· *125*
References ····· *127*

About This Assessment

This report systematically assesses the digital sovereignty development status of BRICS countries and BRICS+ expanded member countries based on the Digital Sovereignty Index (DSI) framework. The assessment process, jointly facilitated by the Global South Academic Forum and IDEAS, employs a structured multi-agent collaborative system to ensure comprehensiveness in data collection, objectivity in evidence evaluation, and reliability of analytical conclusions.

Assessment Process

For the 11 assessed countries (China, Brazil, Russia, India, South Africa, United Arab Emirates, Egypt, Ethiopia, Iran, Saudi Arabia, Indonesia), the assessment team systematically collected and analyzed objective evidence regarding each country's policies and regulations, infrastructure deployment, technological capability development, and participation in international rules in the field of digital sovereignty, covering the 4 dimensions and 16 indicators of the DSI framework.

Throughout the entire assessment process, a total of **6,811 pieces** of raw evidence information were collected. After rigorous deduplication, verification, and quality assessment procedures, **5,138 pieces** of high-quality unique evidence were ultimately formed, constituting the empirical foundation of this assessment. This evidence covers various sources including official policy documents from each country, international organization reports, technology deployment data, academic research results, and more, ensuring the comprehensiveness and authoritativeness of the assessment.

During the evidence integration phase, the assessment system assigned confidence ratings (three levels: high, medium, low) and evidence type classifications (policy, regulation, data, analysis, report, case study, etc.) to each piece of evidence and precisely mapped the evidence to corresponding assessment indicators. Through multiple rounds of cross-validation and quality control, it was ultimately ensured that each indicator had sufficient evidence support, laying a solid foundation for subsequent quantitative scoring and qualitative analysis.

Scholarly Extension and Global Dialogue

To ensure the empirical findings of this report transition into a sustained academic discourse, the following initiatives have been established as part of this mutual achievement:

Journal Theme Collection: In collaboration with the international journal AI & Innovation (published by Wiley), a dedicated theme collection (Sovereign AI and Digital Sovereignty) has been launched. This provides a peer-reviewed platform for researchers to build upon the DSI dimensions—Data, Infrastructure, Governance, and Capability.

Online Seminar Series: The IDEAS Center for South Asia & Middle East Studies will host a series of online seminar panels to discuss the path toward digital autonomy.

ZGC Forum Release: This report and its accompanying academic roadmap are released at the 2026 Zhongguancun Forum to promote cognitive consensus and pragmatic cooperation among the Global South.

Assessment Methodology

The assessment adopts a five-level maturity model: **Level 1-Initial**, **Level 2-Aware**, **Level 3-Developing**, **Level 4-Competent**, **Level 5-Independent**. Each indicator is independently scored based on collected evidence, dimension scores are calculated as the arithmetic mean of scores of their constituent indicators, and

the national total score is derived from the arithmetic mean of the four-dimension scores.

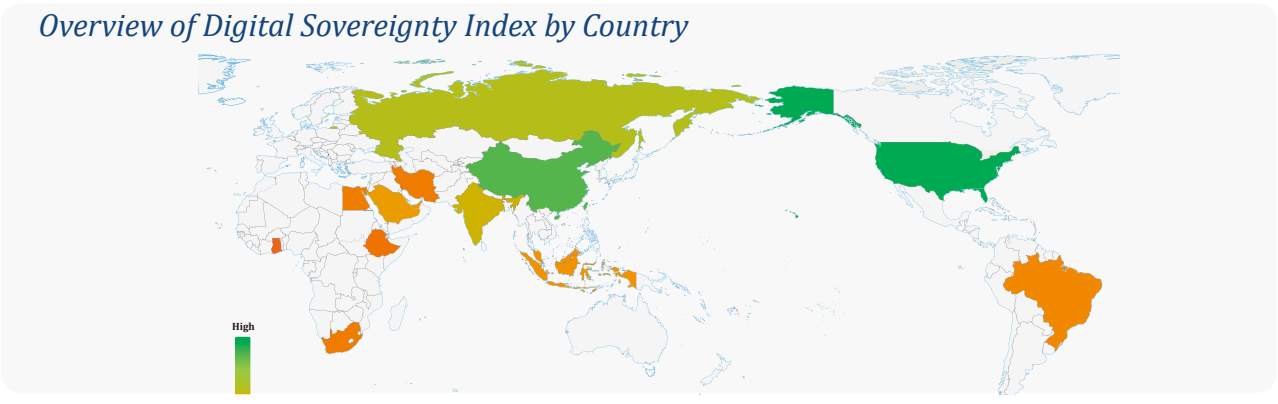
This assessment adheres to the principle of objectivity, with all scores based on verifiable public evidence, avoiding subjective speculation. At the same time, the assessment fully considers the differences in national conditions, and on the basis of unified standards, conducts fair evaluations of countries at different development stages and with different strategic choices.

Assessment Findings

This assessment reveals that the digital sovereignty development of BRICS countries and BRICS+ expanded member countries exhibits significant differentiation. China has achieved relatively comprehensive results in digital sovereignty construction, reaching higher levels in dimensions such as Data Ownership Independence, Digital Infrastructure Independence, Digital Governance Independence, and Digital Capability Independence. Russia demonstrates outstanding performance in Digital Governance Independence and policy frameworks but still faces challenges in the independence of foundational hardware. India, with its vast digital talent pool and active local technology ecosystem, shows strong capabilities in the Digital Capability Independence dimension, but still needs to strengthen in data ownership and infrastructure independence. The digital sovereignty development levels of other BRICS+ expanded member countries (Brazil, South Africa, United Arab Emirates, Egypt, Ethiopia, Iran, Saudi Arabia, Indonesia) vary considerably, with most countries still in the initial or developing stages in areas such as digital infrastructure, core technology independence, and participation in international rules. This disparity reflects not only the different resource endowments, development stages, and strategic priorities of each country, but also highlights the common challenges faced by Global South countries on the path of digital sovereignty construction.

The current global digital space exhibits an extremely unbalanced power structure. The United States and its allies, by virtue of first-mover advantages and technological monopolies, occupy dominant positions in key areas such as internet infrastructure, core technology standards, and data flow rules, forming systematic digital hegemony. For the vast majority of Global South countries, the absence of digital sovereignty not only means a passive position in the distribution of digital economy dividends, but also concerns national security, cultural identity, and the autonomy of development paths. From the "Arab Spring" to hybrid warfare against Latin American countries, from mass cyber surveillance to unilateral supply cutoffs of critical infrastructure, digital space has become a new battlefield for great power competition and geopolitical rivalry. In this context, enhancing digital sovereignty levels, reducing excessive dependence on external technologies and platforms, and conducting digital sovereignty collaboration at regional and global levels have become urgent issues for Global South countries to safeguard national sovereignty, guarantee development rights, and achieve sustainable development. By systematically assessing the current state of digital sovereignty in BRICS countries and BRICS+ expanded member countries, this report paper aims to provide objective reference basis for policymakers, researchers, and stakeholders in each country, promoting cognitive consensus and pragmatic cooperation in the field of digital sovereignty among the Global South.through its associated journal collections and international seminar series.

Overview of Digital Sovereignty Index by Country



For more information, please visit:

https://dsi-online.org/

https://thegsaf.org/

https://ideas-brics.org/

Digital Sovereignty from a Global South Perspective: National Attitudes and Measurement Systems

The Chinese version of this article was published in Jinan Journal (Philosophy and Social Sciences Edition). Citation information:

Xiong Jie. Digital Sovereignty from a Global South Perspective: National Attitudes and Measurement Systems. Jinan Journal (Philosophy and Social Sciences Edition). 2025, 47(8): 13-35

I. The Rise of the Concept of Digital Sovereignty

In 2013, former CIA employee Edward Snowden handed a classified document to The Guardian in the United Kingdom, exposing the world-shocking "PRISM" scandal. When then-President of Brazil Dilma Rousseff learned that the commercial secrets of Petrobras and all her internet records were being monitored by the U.S. National Security Agency (NSA), she angrily canceled her state visit to the United States. Three years later, Rousseff was impeached, with the cause being the so-called corruption case involving Petrobras.

Also in 2013, another female leader who learned through the PRISM scandal that she was being monitored by the NSA, then-German Chancellor Angela Merkel, vowed to push for stricter EU data protection rules. Three years later, Europe released the General Data Protection Regulation (GDPR), touted as "the strictest data protection legislation in history." Wired magazine believed this law "would set the tone for global data protection for the next decade." (Although a few years later, another Wired article asked "How GDPR Failed," which this paper will discuss later.) In 2020, when Germany assumed the rotating presidency of the Council of the European Union, it proposed that "Europe must strengthen its digital sovereignty to effectively respond to future challenges, secure livelihoods, and ensure citizens' safety." The concept of "Digital Sovereignty" thus began to attract widespread attention from academic, industrial, and policy research communities worldwide.

There are several slightly different versions of the definition of digital sovereignty. For example, the French IT consulting company Atos defines digital sovereignty as a combination of "data sovereignty" and "technology sovereignty," subdivided into three levels: geographical location, operations, and regulatory rules; Chinese scholars Zeng Jingjing and others have added the dimension of "cyberspace sovereignty" on this basis. However, most researchers agree on a broad definition: digital sovereignty is the extension of state sovereignty under the Westphalian system into digital space. This system's definition of sovereignty includes three core elements: sovereign states have sovereignty over their territory and domestic affairs, excluding all external interference; states mutually recognize each other's sovereignty and do not interfere in each other's internal affairs; the sovereignty of all states (regardless of size or strength) is equal. Since digital space both overlaps with and differs from the national borders of the physical world, sovereignty claims in the physical world will inevitably affect jurisdiction in digital space; conversely, overemphasizing the openness of digital space will create "arbitrage" phenomena that damage state sovereignty in the physical world. Thus, the existence of digital sovereignty is an objective reality, with the only question being the extent and manner in which states assert their digital sovereignty.

The role of state sovereignty in digital space governance has historically been a controversial issue. In 2001, the United Nations approved the convening of the World Summit on the Information Society (WSIS) in Resolution 56/183. By 2003, as discussions deepened, WSIS had effectively evolved into a World Summit on Internet Governance. As an UN-mandated conference, WSIS should have been a platform for intergovernmental organizations to participate in internet governance, with member states serving as the most important, or even sole, actors in internet governance processes. This was also the prevailing view of most developing countries. However, the United States insisted that internet governance should be dominated by private enterprises. Under pressure from the U.S. side, WSIS established a "multi-stakeholder" governance model after meetings in Geneva and Tunis, stating that "the international management of the internet should… involve the full participation of multiple stakeholders including governments, the private sector, civil society, and international organizations."

Although consensus on the multi-stakeholder principle was reached, countries actually had different understandings of its actual content. Countries such as Brazil, Russia, and China believed that the internet is a public resource (similar to natural resources) and should be managed primarily by national governments, with other stakeholders serving only as auxiliary roles providing advice and oversight. American scholars believed that these countries were "merely reaffirming traditional governance models," suppressing the voices of stakeholders beyond government. However, the reality is that the United States strongly promoted the multi-stakeholder model primarily to facilitate its domestic tech companies becoming "first-class citizens" in international digital space governance. As scholars such as Shen Yi have pointed out, organizations such as the Internet Corporation for Assigned Names and

Numbers (ICANN) and the Internet Engineering Task Force (IETF), which are very important in international internet governance, are actually highly controlled by the U.S. government. Those participating in WSIS discussions as "civil society representatives" were basically "cosmopolitans and transnational activist elites among international NGO staff"—most funded by international development agencies from Europe and the U.S., such as the U.S. Agency for International Development (USAID). Granting these non-governmental stakeholders equal voice with national governments is essentially weakening the voice of national governments in digital space governance.

Of course, completely transplanting the multilateral international relations model of the physical world to digital space governance would also have problems. Although the state-centric governance philosophy and hierarchical power structure contained in this governance model can ensure the realization of national interests in the internet field, its greatest deficiency is that state-centric governance philosophy leads to internet fragmentation and balkanization. Therefore, the ideal model for digital space governance should promote communication, interaction, mutual benefit, and win-win in global digital space on the premise of respecting the equality of national sovereignty (including sovereignty in digital space) and respecting the independent choice of digitalization development paths by all countries. This is the basic position of our government on international cyberspace governance and the basic starting point for this paper's research on digital sovereignty.

Additionally, some researchers approach the issue from the perspective of individual internet users, discussing "personal digital sovereignty" (mainly referring to ownership and usage rights of personal data), and have developed technical solutions such as Solid. However, this branch has had relatively little real-world impact overall. There are also some discussions about "corporate digital sovereignty," mostly about how companies respond to the major trend of increased emphasis on national digital sovereignty. The main content of this paper is national digital sovereignty, and does not pay much attention to the latter two types of discussion.

This paper will first introduce how countries around the world currently approach the concept of digital sovereignty based on their respective capabilities and interests. In fact, except for the United States, which holds comprehensive hegemony in digital space, all other countries and regions recognize the importance of national digital sovereignty. However, due to constraints on their capabilities and endowments, countries' levels of striving for digital sovereignty vary. Particularly, Global South countries (excluding China) lag relatively behind in both digital technology capabilities and digital space governance capabilities and generally find it difficult to strive for and maintain their own digital sovereignty. Today, contradictions between the Global North developed countries led by the United States and the Global South are becoming increasingly acute. The Global North relies more heavily on neocolonial plunder of Global South countries due to its own industrial hollowing out, and hegemony over the digital economy and digital space is precisely an emerging area of this parasitic plunder. Therefore, protecting digital sovereignty has become an urgent challenge for the vast majority of Global South countries. The first step for countries to address this challenge is to establish a comprehensive understanding of digital sovereignty and an objective understanding of their own digital sovereignty status.

However, the harsh reality is that there is currently no relatively comprehensive method for measuring digital sovereignty internationally, let alone a systematic assessment of the digital sovereignty levels of Global South countries. As readers will see later, although some research institutions have separately proposed methods for measuring national digital independence and autonomy capabilities, these methods all have significant limitations and are insufficient to provide policy references for the digital sovereignty strategies of numerous Global South countries. In response to this situation, the author proposes a digital sovereignty measurement system starting from four dimensions: data ownership, digital infrastructure, digital space governance, and digital capability, which can relatively clearly assess countries' levels of independence and autonomy in these four dimensions, thus providing references for policies to enhance the digital sovereignty levels of Global South countries. Considering that most Global South countries' digital sovereignty strategies are still in their early stages, and that most countries objectively cannot build a relatively complete digital industry chain within their own borders, they must seek to enhance their digital sovereignty levels within the framework of global and regional cooperation. The measurement system proposed by the author will also help countries incorporate digital sovereignty into consideration when engaging in international cooperation.

II. Different Approaches to Digital Sovereignty Among Countries Under the North-South Pattern

Compared to the physical sense of "territory," digital space has no physical borders, and countries' digital behaviors intermingle with each other, while being highly dependent on technology. Based on these characteristics, countries have different claims and actions regarding the concept of "extending state sovereignty to digital space," especially the concept of "excluding all external interference" in digital space. The Global North developed countries with strong digital capabilities (including technical and governance capabilities) all have strong digital sovereignty awareness, but this awareness manifests as different policy behaviors in the United States and Europe; China and Russia, from the perspectives of national security and geopolitics, have been forced to emphasize digital sovereignty, each achieving relatively significant results; other Global South countries' attitudes toward digital sovereignty cannot be generalized, and their development levels are also uneven, but from countries' actions, some common demands for digital sovereignty can already be seen.

As the pioneer and absolute leader in digital technology, American researchers generally tend to emphasize the openness of the internet and use this to argue that the concept of state sovereignty does not apply to digital space. A representative view holds that "the internet consists of open-source software protocols that no one owns, and thus no one can exercise exclusive power over them," and further argues that advocating for digital sovereignty equals "calling for an end to global free trade in software, information services, and ICT equipment, and instead supporting ICT self-sufficiency," or even "partitioning or fragmenting the global internet into national territories." Given that the vast majority of internet users worldwide (excluding China) are locked into platforms provided by several tech giants located in the United States and deeply cooperating with the U.S. government, this opposition to digital sovereignty is actually equivalent to proposing to maintain the status quo of U.S. exclusive control over the internet. The 2020 World Economic Forum also proposed that "governments only need remote access to corporate-owned data, and where the data is stored doesn't matter," in other words, maintaining the status quo where the vast majority of Global South countries hand over all their data to American tech giants.

The basis for American institutions and researchers opposing the concept of digital sovereignty is this status quo: the United States already possesses the most powerful digital sovereignty, other countries can hardly violate U.S. digital sovereignty, and the United States can use its digital hegemony to continuously erode other countries' sovereignty. What they call "opposing digital sovereignty" is actually a subtext of "opposing countries other than the United States having digital sovereignty." However, with China's rapid development in digital technology, this status quo is facing challenges. In recent years, the U.S. government has frequently used trade control tools such as the "Entity List" to restrict exports of key technologies (especially chips) to Chinese tech companies such as Huawei, issued bans or promoted forced divestiture bills on Chinese-backed applications such as TikTok and WeChat in the name of national security, supported the domestic semiconductor industry and squeezed out competitors through industrial policies such as the CHIPS and Science Act, and even pressured allies to exclude specific Chinese suppliers in 5G network construction. Faced with the U.S. government's clearly targeted protectionist policies against foreign digital tech companies, these institutions and researchers advocating for "borderless digital space" have not raised criticisms. This shows that although they claim to advocate for the openness of digital space, their true purpose is to maintain the hegemonic position of the United States.

Although both belong to the Global North developed country camp, Europe's reality differs from the United States: Europe has a strong digital technology industrial base, but in the internet era, these companies are suffering fierce competition and suppression from American counterparts who have mastered the advantage of scale; the loss of industrial positions has further caused Europe to lose its dominance in the control and governance of digital space. Therefore, European political leaders view the concept of digital sovereignty as a means to promote Europe's leadership and strategic autonomy in the digital field. After fully implementing the privacy and data protection framework centered on GDPR, the EU's main measures to strengthen its digital sovereignty currently include: establishing a legal and infrastructure framework for data collection, data processing, and data sharing within the EU; establishing a certification and procurement framework

for digital systems based on trustworthiness; and establishing a complete set of protection mechanisms for European tech companies. Europe still has considerable technological and talent accumulation, and the above measures are mainly intended to protect and revitalize domestic enterprises and seek to rebuild Europe's industrial competitiveness in the digital age.

It is worth noting that the EU's digital sovereignty strategy is not merely defensive inward. A significant feature of a series of high-standard digital regulations represented by GDPR (also including the Digital Markets Act, Digital Services Act, Artificial Intelligence Act, etc.) is their broad extraterritorial effect—these regulations apply not only to companies operating within the EU but also to companies outside the EU that provide products or services to EU citizens. This practice of imposing its own legal standards on global digital service providers essentially uses its huge unified market as leverage to export EU rules and values globally, shaping the landscape of global digital governance. Some analysts interpret this as the EU attempting to make itself "a strategically autonomous third-pole force" independent of China and the United States through "normative power," thereby enhancing its global influence. From the perspective of sovereignty practice, this strategy is essentially an outward expansion of sovereignty, maintaining and extending its own interests and influence by setting global standards, which is essentially no different from the United States using technological hegemony and long-arm jurisdiction to push its claims, both reflecting the reality of Global North developed countries actively using various means to consolidate and assert their digital sovereignty.

It can be seen that although the United States and Europe adopt different action strategies, they actually both have strong digital sovereignty awareness. Global North developed countries have a clear understanding of the exclusivity and complexity of digital sovereignty. On the one hand, they protect their own digital sovereignty, and on the other hand, they seize every possible opportunity to extend the scope that their digital sovereignty can cover and govern—the United States using domestic law to govern the global operations of its internet platforms goes without saying, and Europe's GDPR also extends its jurisdiction to digital platforms worldwide that serve European citizens, regardless of where their corporate entities or servers are located. Compared to them, the digital sovereignty awareness of China, Russia, and other Global South countries has largely been formed passively under the pressure of the Global North camp. The historical roots of this reaction can be traced back to the post-colonial era's vigilance against Western information hegemony under the slogan of "free flow of information" (such as the call for "cultural sovereignty" in the NWICO debate), and in contemporary times has been continuously strengthened in response to the United States' technological monopoly (and the accompanying risk of "digital colonialism"), cyber surveillance (as revealed by the PRISM scandal), geopolitical intervention (such as color revolutions), and ideological infiltration. Therefore, understanding these countries' state-centric digital sovereignty construction cannot be separated from their relatively weak and passive position in the global power structure, as well as their realistic needs to maintain national security, cultural identity, and autonomy in development paths.

China began vigorously developing the electronics and information industry from the late 1990s, initially being completely open to Western, especially American, tech companies. During the same period, China's nascent internet imposed no restrictions on American companies. However, as the internet's influence on public opinion and politics gradually became prominent, especially with the continuous deepening of Western ideology in Chinese society, the autonomy of digital space construction and governance received attention from the Chinese government. Chinese political philosophy does not recognize a "virtual world" separate from the physical world; the state's sovereignty and governance naturally extend to digital space. After Donald Trump was elected president in 2016, the United States strengthened its technological constraints on China, and China further accelerated its pace toward information technology independence and autonomy, conducting a series of legislation in areas such as cybersecurity, privacy protection, and anti-monopoly, and accelerating the domestication of information technology products through mechanisms such as "Xinchuang" (Information Technology Innovation). Particularly noteworthy is that in 2019, the Fourth Plenary Session of the 19th CPC Central Committee first proposed treating data as a new type of production factor, thus pioneering the quantification, monetization, and nationalization of data value, and presciently bringing the digital economy under the scope of national sovereignty jurisdiction.

Russia has traditionally emphasized establishing the principle of state sovereignty in the ICT field through international political channels. Since 1998, Russia has

repeatedly promoted initiatives to safeguard international information security within the UN, regional organizations, trans-regional organizations, and bilateral cooperation frameworks, based on the principle of sovereign equality of states at the international law level. A series of color revolutions such as the "Arab Spring" that occurred in the 2010s prompted Russia to further reduce domestic industries' dependence on foreign technology, construct, develop, and expand the use of its own equipment, and form production and services on this basis. In November 2019, Russia passed the Sovereign Internet Law, providing a legal basis for centralized internet management within its borders. The special military operation that began in 2022 and the deterioration of relations with Western countries prompted Russia to continue strengthening policies in the field of digital sovereignty. Sanctions pressure from Western countries also prompted Russia to reduce dependence on foreign countries in the information technology field, and some domestic internet applications began to emerge.

As mentioned above, as the main geopolitical adversaries of the United States and NATO, China's and Russia's emphasis on digital sovereignty is largely a defensive measure against pressure imposed by Global North developed countries, especially the United States. In the process of responding to the United States' continuously escalating hybrid warfare tactics and protecting their own national security, these two countries have formed relatively comprehensive views on digital sovereignty. Thanks to their deep industrial, technological, and educational foundations, China and Russia have been able to establish relatively complete digital sovereignty systems (Russia still has obvious shortcomings in basic hardware autonomy).

Apart from the two major powers of China and Russia, the Global South is difficult to discuss as a whole: Brazil, India, South Africa, Saudi Arabia, and Singapore each have their own views on national digital strategy and digital sovereignty, and there is no so-called "Global South digital sovereignty view." However, Global South countries (excluding China) do share a common feature: their digital technology capabilities overall—compared to Europe, Russia, and China—are relatively weak, and they are temporarily unable to widely replace the digital infrastructure dominated by the United States. Nevertheless, India and Brazil are still striving to break free from comprehensive dependence on U.S. digital applications and digital infrastructure. More economically developed countries with closer relations to the United States, such as Saudi Arabia and Singapore, place more emphasis on how to keep the economic dividends brought by digitalization within their own countries, rather than replacing U.S. digital infrastructure. Compared to them, most African countries have a very low level of awareness of digital sovereignty, and discussions about "the need to be vigilant about American tech giants" have only recently begun to emerge, with digital sovereignty not yet becoming a focus of attention for most African governments.

Synthesizing the digital sovereignty views of countries outside the United States, we can see that countries' actions and demands are concentrated in the following areas:

1. Protecting national security from threats in digital space. The United States' hegemony in digital space (excluding China) has become a concentrated embodiment of what Samir Amin called imperialism's monopoly on information and communication under new technological conditions. From the Arab Spring in the early 2010s, to a series of hybrid warfare measures against Cuba, Venezuela, and Brazil, to the riots that occurred in Hong Kong, China in 2019, to the disappearance of Iranian state media websites from DNS root nodes in 2021, to Russian content being restricted or even blocked on mainstream social media platforms after the start of special military operations in 2022, digital space is clearly no longer a purely virtual space unrelated to real state sovereignty. Countries around the world, especially Global South countries, need to worry that the network platforms and data controlled by the United States will suddenly become weapons threatening national security and sovereign independence. In fact, while persuading other countries not to restrict the internet, the United States restricts and attacks Chinese companies and products such as Huawei, ZTE, WeChat, and TikTok for national security reasons.

2. Mastering digital economy autonomy and ensuring that the country and its citizens enjoy digital dividends. One estimate used by the World Economic Forum believes that the digital economy's contribution to global GDP exceeds 15%, or more than $15 trillion (2022). Another estimate believes that 70% of the new value created by global economic activities in the next decade will be based on digital platform business models. China's estimate is that more than 40% of its GDP is related to the digital economy. With such enormous economic volume,

can the country and its citizens obtain the main benefits, or should they allow American tech giants to extract large amounts of economic value from it? Some researchers call the behavior of American tech giants extracting digital economic value from the Global South "digital colonialism." In recent years, China has gradually promoted the quantification of the economic value of data and its inclusion in corporate balance sheets, making the analogy of "digital colonialism" more concrete: data itself is an "asset" with economic value (just like minerals), and because the United States has a firm monopoly position at multiple levels including hardware, software, applications, and cloud, the data assets of most Global South countries are extracted by American tech giants by default.

3. Ensuring law enforcement rights in digital space and protecting citizens' digital rights. Although all countries claim to agree with the principles of openness, freedom, and equality on the internet, when it comes to specific issues, different cultures, traditions, and customs of different countries, civilizations, nations, and religions determine that there cannot be a unified "digital space value system" for the entire world. What is legal behavior in one country may be illegal in another. Additionally, the "borderless" nature of the internet also makes it more difficult to prevent and punish transnational crimes in digital space. Thus, how to preserve the openness of the internet as much as possible while maintaining the independence of culture, values, and law enforcement rights has become an important demand for Global South countries striving for digital sovereignty. For example, China's "Regulations on Network Protection of Minors" issued in 2023 requires network service providers to provide a minor mode, with strict requirements on the time periods, duration, functions, and content of minors' use of network services, which differs from most other countries' regulatory requirements for internet companies and is a manifestation of state sovereignty in digital space. The U.S. government imposing its domestic law on internet platforms used by countries around the world is essentially its state sovereignty's outward expansion through digital space.

As economic and technological latecomers, most Global South countries are quite weak in national security in digital space, the digital economy, and law enforcement rights in digital space. American tech giants are turning many Global South countries, including South Africa and Brazil, into "digital colonies" of the United States, using their monopoly on digital infrastructure to seize data resources from the Global South, ruling the political, economic, and cultural lives of the Global South through computer-mediated channels, conducting large-scale surveillance in the Global South, and legitimizing their hegemony over the digital world through public opinion and ideology. Therefore, Global South countries need a sense of urgency in striving for digital sovereignty. One particularly noteworthy point is that Global South countries' (including relatively IT-capable countries such as Brazil, India, and South Africa) measures to strive for digital sovereignty remain relatively fragmented and do not reflect a systematic strategic approach. The author believes that the urgent task is to establish a comprehensive measurement system for digital sovereignty that reflects the universal demands of Global South countries, conduct an objective assessment of the digital sovereignty status of Global South countries, and thus provide baselines and references for countries to formulate digital sovereignty strategies.

III. Two Existing Measurement Systems for Digital Space Independence and Their Limitations

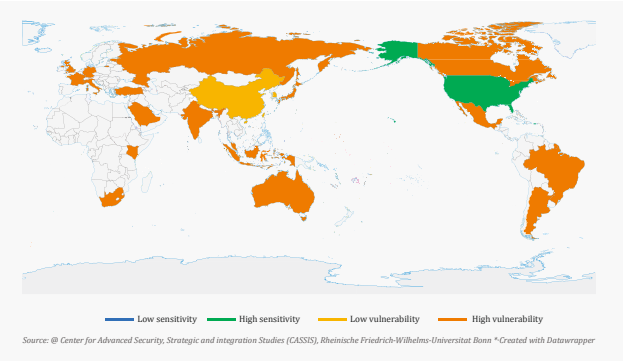
Currently, there is no relatively complete indicator system in the world for measuring the degree of digital sovereignty independence. The University of Bonn in Germany proposed a "Digital Dependence Index," which mainly measures countries' dependence on other countries in the digital field based on indicators such as ICT trade, communication infrastructure, and intellectual property (i.e., ICT-related patents). Several main conclusions drawn from this index can roughly reflect the current degree of digital sovereignty independence of countries around the world:

- The United States has the highest and only digi-

tal independence. Most digital technology is provided by its domestic supply chain.

- China is the only major country outside the United States with relatively high digital independence and relatively less vulnerability to digital supply chain attacks from other countries.

- All other countries are highly dependent on digital technology provided by foreign countries (mainly the United States). Especially, most countries in Asia, Africa, and Latin America are in a state of "absolute dependence."



The "Digital Dependence Index" proposed by the University of Bonn

The deficiency of the Digital Dependence Index is that it focuses too one-sidedly on ICT technology R&D and product manufacturing, ignoring important factors such as data ownership and digital space governance rights, thus producing results that are also one-sided. For example, the index considers South Korea to have digital independence at the same level as China, higher than Japan, India, Brazil, Russia, and Western European countries, which is clearly distorted by the extraordinarily strong R&D and manufacturing capabilities of a few Korean companies such as Samsung.

A study by the National University of Singapore adopted another method for measuring national digital sovereignty levels. This study listed a series of indicator systems related to digital sovereignty and obtained an intuitive understanding of a country's digital sovereignty level through a quick overview of the country's rankings in various indicator systems. This study categorized these indicator systems into four types:

- Cybersecurity. Including the International Telecommunication Union (ITU)'s "Global Cybersecurity Index," Oliver Wyman Forum's "Global Cyber Risk Literacy Index," Estonia's e-Governance Academy's "National Cyber Security Index," and Harvard University's Belfer Center's "National Cyber Power Index."

- Digital economy. Including the Swiss International Institute for Management Development (IMD)'s "World Digital Competitiveness Ranking" and the Portulans Institute's "Network Readiness Index."

- Cross-border data flows. Including Salesforce's "Cross-Border Data Flows Index."

- Data protection and privacy. Including TRPC's "Data Protection Index," DataGuidance's "Privacy Index," and the Global Web Index (GWI)'s "Data Privacy Index."

The advantage of this method is that it can quickly gain a preliminary impression of a country's (in this case, Singapore's) digitalization level, but its disadvantages are also obvious: the various indicator systems are published by different institutions, with different evaluation criteria and scoring methods, and cannot be integrated into one system, nor can adjustments be made to indicator selection and scoring mechanisms. Additionally, the selected indicator systems also reflect Singapore's economic-focused, politics-light characteristics when viewing digital sovereignty issues, ignoring issues such as whether the country's digital infrastructure depends on foreign countries (especially the United States), whether it has independent law enforcement rights in digital space, and even treating cross-border data flows (rather than keeping data and its value within the country) as a positive indicator, failing to represent the demands of many Global South countries for digital sovereignty. Moreover, some of the indicator systems selected in this study show obvious bias. For example, TRPC's "Data Protection Index" ranks China behind Thailand, the Philippines, Vietnam, and other countries, only higher than Laos, Cambodia, and Myanmar. This result clearly deviates significantly from reality. However, because researchers only use the results of selected indicator systems and do not control the specific indicator settings and raw data, they cannot adjust obviously distorted measurement results.

In summary, the research by the University of Bonn and the National University of Singapore has respectively noticed the importance of digital sovereignty and

attempted to establish a relatively concise indicator system to measure the digital sovereignty level of various countries. However, the indicator systems established by both have significant limitations and are not yet sufficient to serve as policy references for Global South countries. Moreover, these two studies expose a deeper challenge: attempting to quickly assess a country's digital sovereignty level through a few indicators (University of Bonn) or by synthesizing the measurement results of a group of existing indicator systems (National University of Singapore) may be difficult to achieve practically meaningful results. The author believes that relevant research on digital sovereignty needs to establish a relatively comprehensive indicator measurement system and conduct measurement and assessment starting from basic data (including both quantitative and qualitative data).

IV. The Necessity and Possibility of a "Digital Sovereignty Index" Based on the Principle of Independence and Autonomy

Starting from the goal of avoiding becoming "digital colonies," the basic principle of Global South countries' digital sovereignty strategies should seek independence and autonomy. On the one hand, independence and autonomy in digital sovereignty does not mean that every country must establish a complete ICT industry chain, but should be comprehensively considered within the framework of regional cooperation and multilateral international cooperation. On the other hand, independence and autonomy in digital sovereignty is not only reflected in the domestication of ICT technology and products or the use of free and open-source software, but should also include legislation, law enforcement, governance, and related capacity building in digital space.

Independent and autonomous data ownership is an issue receiving widespread attention at present. More and more countries are beginning to pay attention to the phenomenon of American tech giants completely seizing data to the United States, and through legislative means requiring that data generated in their own countries be first stored in their own countries, as well as regulating cross-border data transmission. However, independence and autonomy in data ownership is a concentrated manifestation of a country's overall digital sovereignty. If a country does not have independence and autonomy over digital infrastructure (i.e., the hardware and software supporting the operation of digital space), then restrictions on data ownership cannot actually be implemented (this phenomenon was seen in Brazil's case); if a country does not have independence and autonomy in digital governance, then the rules of digital space will inevitably be dominated by American tech giants. And independence and autonomy in digital infrastructure and digital governance both depend on the capabilities of research institutions, enterprises, and talent engaged in the digitalization industry. Therefore, the author believes that a country's digital sovereignty should be reflected in independence and autonomy in the following four aspects:

- Data Ownership Independence. The state should legislate on data ownership, protect citizens' personal data and personal privacy, ensure that data generated domestically is stored domestically, and ensure that sensitive, private, and high-value data generated domestically does not flow abroad without management. The value of data should benefit the people universally, rather than being monopolized by private enterprises (especially foreign private enterprises).

- Digital Infrastructure Independence. Including independence and autonomy in foundational hardware (chips, servers, storage, etc.), foundational software (operating systems, databases, middleware, cloud platforms, etc.), application software (office software, general software, industry software, etc.), and information security.

- Digital Governance Independence. Reflected in domestic digital affairs legislation and law enforcement capabilities, as well as the ability to participate in and lead international digital technology rules and digital behavior rules.

- Digital Capability Independence. Reflected as ICT-related cutting-edge technology R&D capabilities, as well as university-related professional talent cultivation supporting technology R&D, domestic ICT industry engineering technology capabilities, and the level of coordination between digital technology and national development strategies.

This leads to the four dimensions and 16 indicators of the Digital Sovereignty Index (DSI):

1. Data Ownership Independence

1. Legislation on data ownership. The state should enact laws and regulations to protect citizens' data rights (such as the right to informed consent, the right to access and portability of personal information, the right to correction, the right to deletion, the right to restrict processing, and the right to object) from being violated by enterprises operating digital businesses.

2. Domestic data storage. That is, data generated domestically, especially personal information and important data collected and generated during domestic operations in important fields and critical infrastructure such as public communications and information services, energy, transportation, water resources, finance, public services, and e-government, should be stored domestically.

3. Protection of cross-border data transfers. That is, personal information and important data collected and generated during domestic operations of critical information infrastructure should not be arbitrarily extracted by foreign enterprises or flow abroad without regulation, and there should be corresponding legal provisions and management measures.

4. Inclusion of data value for the public. Data is a new type of production factor, and the economic value created by large amounts of data originating from the public should not be monopolized by private internet companies but should benefit society as a whole in some appropriate manner.

2. Digital Infrastructure Independence

1. Independence of foundational hardware. Mainly including chips, servers, storage devices, and other hardware constituting the physical foundation of digital space, to what extent it can be independently autonomous and controllable.

2. Independence of foundational software. Mainly including operating systems, databases, middleware, cloud platforms, and other software foundations for digital business and digital economy operations, to what extent it can be independently autonomous and controllable.

3. Independence of application software. Mainly including office software, general software, industry software, and other application software with large usage volumes and close relationships with economic production, to what extent it can be independently autonomous and controllable.

4. Independence of information security. That is, the degree to which the country is independently autonomous and controllable in the field of information security and network security, including the level of independence and autonomy in technology, legislation, and facilities.

3. Digital Governance Independence

1. Legislative capacity for digital affairs. That is, the country's ability and level of independence and autonomy in legislation in various digital affairs fields, especially how to respond through legislation to some common challenges in the digital economy that the whole world faces (such as platform monopolies, information cocoons, protection of labor rights in the platform economy environment, etc.).

2. Enforcement capacity for digital affairs. That is, the country's ability to implement legislation in the digital field, especially the ability and determination to regulate large platforms and large enterprises, and severely punish and combat illegal behavior.

3. Leadership in international digital technology rules. That is, the influence and leadership of the country and its enterprises in the process of formulating international digital technology rules. An important indicator is the voting seats held by the country's government and enterprises in major international standardization organizations.

4. Leadership in international digital behavior rules. That is, the country's influence and leadership in international cooperation and international governance in the digital field, especially the ability to propose claims and build consensus on issues of common concern such as international cooperation in digital trade, cross-border data flows, and global digital governance.

4. Digital Capability Independence

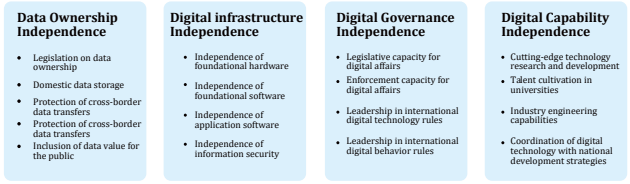
1. Cutting-edge technology research and development. That is, the quantity and quality level of the country's scientific research and innovation in digital industry-related technical fields such as

electronics, communications, and information. An important indirect indicator is the number of international patents granted under Category I "Electrical Engineering" of the World Intellectual Property Organization (WIPO) (including 5 subcategories: 1. Electrical machinery, apparatus, energy; 2. Audio and video technology; 3. Telecommunications; 4. Information technology; 5. Semiconductors).

2. Talent cultivation in universities. That is, the quantity and quality of high-level talent trained in professional fields related to the digitalization industry, one important indicator being the total number of university graduates in science, technology, engineering, and mathematics (STEM) disciplines.

3. Industry engineering capabilities. That is, the country's ability to convert scientific research results into engineering technology implementation in digitalization-related fields such as information and communication, software and information technology services (including enterprise capabilities and practitioner capabilities), as well as the level of independence and autonomy of digital industry engineering technology capabilities.

4. Coordination of digital technology with national development strategies. That is, the extent to which the country's technological development in electronics, information, communications, digitalization, and other fields resonates and mutually enhances with the development strategies in national defense, economy, culture, people's livelihood, and other fields, rather than being dominated by other countries (especially Western developed countries).



The 4 dimensions and 16 indicators of the Digital Sovereignty Index

The rating for each indicator ranges from 1 to 5, respectively marking the country's degree of independence and autonomy in the field represented by this indicator from low to high:

Level 1: Initial—The country has not yet treated independence and autonomy in this field as an issue to address.

Level 2: Aware—Beginning to realize the importance of independence and autonomy in this field and starting relevant discussions and actions.

Level 3: Developing—Already gradually developing independence and autonomy in this field, having achieved certain results, but still having a large gap from breaking free of external dependence.

Level 4: Competent—Already having quite strong international competitiveness in this field, having considerable independence and autonomy, and already possessing the potential to rapidly develop into complete independence and autonomy when necessary.

Level 5: Independent—Basically completely independent and autonomous in this field, with relatively small constraints and threats from external dependence.

The 5 levels of the Digital Sovereignty Index

V. DSI Assessment Methodology and Examples

DSI-based assessment and measurement currently mainly adopts a mixed qualitative and quantitative assessment method, combined with expert consultation methods to review and correct biases in assessment. First, the author conducts extensive desk research to systematically collect publicly accessible information from various channels, including: reports and analytical articles from news media; industry reports from market research companies and industry associations; legal documents, regulations, and policy documents related to fields such as data management, cybersecurity, and digital infrastructure; academic articles and

research papers studying countries' ICT industries and digital policies. Based on this comprehensive investigation, the author categorizes qualitative or quantitative information according to the 16 indicators of DSI, thus forming assessment conclusions for each indicator.

For some indicators in the DSI framework, relatively representative and highly quantified indirect indicators can be obtained. For example, for indicator 3.3 "Leadership in international digital technology rules," it is possible to count the proportion of voting seats held by the country in 11 relatively important international standardization organizations (SDOs) in the ICT field, thus relatively accurately obtaining knowledge of the country's influence in the formulation of international digital technology rules. Taking the countries for which the author has completed assessments as examples, of the 2,610 voting seats in these 11 SDOs, the United States holds 818 seats, accounting for 31.34%; China holds 286 seats, accounting for 10.96%; Brazil holds only 20 seats, accounting for 0.77%. From this, the author concludes: the United States' rating on this indicator is "Level 5: Independent"; China's is "Level 3: Developing," meaning that it has achieved certain results in this field but still has a considerable gap from the world's advanced level; Brazil's is "Level 2: Aware," meaning that relevant actions are still in the early stages and have not yet achieved significant results. Another example is indicator 4.2 "Talent cultivation in universities," which can be indirectly reflected by the total number of university graduates annually in science, technology, engineering, and mathematics (STEM) disciplines in the country. This will not be elaborated further here.

However, it must be admitted that for most indicators in the DSI framework, simple, quantified indirect indicators do not yet exist, and can only be done through comprehensive analysis of relevant information and horizontal comparative assessment from an expert perspective, evaluating a country's level of independence and autonomy on each indicator in this way. The definition of indicator ratings (from 1 to 5) also reflects the objective reality that the assessment process is more qualitative than quantitative: it does not attempt to give very precise quantitative conclusions for each indicator, but rather qualitatively describes the country's overall situation in a certain aspect from a macro perspective, pointing out general directions for further in-depth research and policy formulation.

Below, the author will use the assessment process for Brazil on indicator 1.3 "Protection of cross-border data transfers" as an example to illustrate the assessment method for relatively qualitative indicators in the DSI framework.

The author first searched for information on Brazil's legislation and law enforcement related to cross-border data flows from various information sources. The author learned that Brazil's main data protection legislation is the General Data Protection Law (LGPD), which came into effect in 2018 and includes a chapter on international data transfers; in addition, Federal Law No. 12965/2014 and its Decree No. 8771/16 (collectively called the "Brazilian Internet Law") also impose requirements on service providers, network and application providers regarding the processing of personal data and other obligations. Further study of the relevant legal provisions reveals that LGPD made relevant provisions on cross-border transmission of personal data, and the law enforcement agency responsible for implementing LGPD, the National Data Protection Authority (ANPD), also issued corresponding management regulations and standard contract clause templates. However, on the other hand, no coercive measures have yet been seen taken by law enforcement agencies against behavior violating LGPD (including non-compliant cross-border data transmission), so relevant researchers generally believe that the actual enforcement strength of LGPD remains to be seen. Based on this information, the author believes that Brazil has the intention to protect data resources produced within its borders from flowing out freely, and is also gradually advancing legislative regulation. This indicator should be rated as "Level 2: Aware," meaning that the country has become aware of the importance of protecting cross-border data transmission and has begun to take relevant actions (although the actions are still in the early stages and no results have been seen yet).

Subsequently, the author sent the draft assessment report to Brazilian expert Sergio Amadeu, former director of the Brazilian National Institute of Information Technology, for comments. Amadeu pointed out that the actual situation of Brazil's cross-border data transmission protection is worse than what the author researched and understood. Due to the political influence of the financial sector and big tech companies, the detailed implementation work on cross-border data transmission has actually been shelved, and data within Brazil continues to flow abroad without regula-

tion. Based on Amadeu's input, the author adjusted the assessment result for this indicator to "Level 1: Initial," meaning that the country has not actually treated the protection of cross-border data transmission as an important matter to value and promote.

From the above case, it can be seen that the DSI assessment process inevitably has considerable subjectivity. Given the reality that Global South countries generally have low digitalization levels and weak national basic capabilities (such as national economic statistics, government transparency, etc.), most indicators involved in DSI, in most countries, do not have ready-made, clearly quantified information published. At the present stage, initial and overall understanding of the digital sovereignty levels of various countries can only be formed based on qualitative research and analysis based on expert experience, and attempts made to minimize bias and misjudgment through cooperation with local experts. As mentioned earlier, some existing studies (such as the research by the National University of Singapore) attempt to integrate the ratings and scoring results of multiple research institutions to form a seemingly quantified comprehensive assessment, but its results deviate significantly from reality, and subsequent researchers cannot revise and improve on its basis. In comparison, although DSI's assessment method has coarse granularity, is more qualitative than quantitative, and has obvious subjectivity, the raw materials and rating methods it uses are disclosed in the assessment report, both providing directional guidance for policymakers and creating possibilities for subsequent researchers to participate in improving assessment conclusions.

The research work the author is currently conducting is using the DSI measurement framework to assess and measure the digital sovereignty levels of BRICS countries, establishing quantified baselines for each country's digital sovereignty, so as to subsequently provide references and recommendations for work to enhance countries' digital sovereignty levels on this basis. Looking comprehensively at the DSI assessment results for various countries in the BRICS organization, an increasingly clear conclusion is: for the vast majority of Global South countries, including countries like India that have huge markets and talent reserves, in the current global digital political-economic landscape dominated by a few Northern countries and their tech giants, trying to accumulate a complete ICT industry system entirely through self-reliance, cultivate sufficient talent echelons, and ultimately achieve comprehensive digital sovereignty independence and autonomy has become extremely difficult, or may even no longer be a realistic and feasible path. The Global South may need to seek another path to obtain digital sovereignty, such as working closely with China and Russia within the BRICS framework to establish an alternative digital infrastructure suitable for the Global South that respects the digital sovereignty of all countries, and build the talent and enterprise capabilities of various countries around this plan. Realizing this vision requires a great deal of international cooperation and requires proposing a revolutionary international digital space governance system. Governments and scholars of Global South countries need to start thinking about this issue now and promote the formation of the Global South's digital sovereignty strategy.

Summary and Outlook

From "PRISM" to the blocking of Iranian news websites on DNS root servers, from color revolutions in Syria to the suppression of pro-Palestinian voices on mainstream social media platforms after "Al-Aqsa Flood," the myth of an "open, free, and equal" internet long cultivated by the United States has accelerated its collapse over the past decade or so. Global North developed countries have proven through their actions that they value their own digital sovereignty and are working hard to defend and expand the coverage of their Westphalian sovereignty in digital space. At the same time, Global South countries generally have not yet formed a comprehensive concept of digital sovereignty. However, Israel's large-scale explosive attacks on Lebanon through communication tools such as pagers and walkie-talkies under its manipulation are enough to make the vast majority of Global South countries realize that: lacking an independent, autonomous, reliable,

and trustworthy supply chain for information technology and digital technology means serious loss of state sovereignty in today's highly digitalized world. A few countries such as China and Russia have established relatively independent digital sovereignty systems under geopolitical pressure, and their experiences will serve as references for other Global South countries.

In order to present a country's level of digital sovereignty independence and autonomy more comprehensively and intuitively, the author designed the Digital Sovereignty Index (DSI) as a measurement indicator system. Through analysis of the DSI assessment results for a series of countries, it is found that for most Global South countries, seeking independence and autonomy in digital sovereignty is a daunting task, and is difficult, or even no longer possible, to complete through a country's own efforts. However, independence and autonomy in digital sovereignty does not mean that every country must establish a complete ICT industry chain—and in fact, it is not possible. The digital sovereignty independence movements of Global South countries—like the national independence movement represented by the Bandung Conference—will inevitably be an internationalist movement, with regional development plans in various regions and multilateral international cooperation mechanisms including China and Russia all playing important roles in it. The goal of the Digital Sovereignty Index is to provide references for countries while providing a common dialogue baseline in these international cooperation mechanisms.

In response to the inadequacies of existing measurement systems and the urgent need for Global South countries to enhance digital sovereignty, the Digital Sovereignty Index (DSI) proposed by this research aims to bridge the gap between theory and practice, providing intellectual support for the autonomous development of Global South countries in the digital age.

First, DSI, as a standardized analytical framework, provides a "common language" for assessing the current status of digital sovereignty in various countries. Through its four dimensions and sixteen specific indicators, countries can systematically examine their strengths and weaknesses in data ownership, digital infrastructure, digital governance, and digital capabilities, thus laying a foundation for formulating precise and effective national digital strategies.

Second, the value of DSI lies not only in assessment but also in promoting cooperation. Based on comparable assessment results, Global South countries can more clearly identify common challenges faced and complementary strengths, providing objective bases and entry points for effective policy dialogue, experience sharing, and practical cooperation (such as in technical standards, infrastructure construction, talent cultivation, etc.) in the field of digital sovereignty.

Furthermore, the application and development of DSI is an open and pluralistic process that requires the participation and contribution of multiple actors. Academia can verify, revise, and enrich the indicator system through continuous research, enhancing its scientific nature and applicability; government decision-makers in various countries can use it as a reference tool for formulating national digital policies and participating in international digital governance negotiations; international cooperation platforms (such as the BRICS mechanism and regional development organizations) can use DSI to promote relevant agendas, coordinate member state positions, and jointly shape a fairer and more reasonable global digital order; the industry and civil society organizations can also refer to DSI assessment results to clarify their positioning and responsibilities in national digital sovereignty construction.

The DSI has been proposed for only a short time, and exchanges with academic and policy communities in various countries have just begun. The author is actively promoting exchanges and application of DSI within the Global South through the international academic platform "Global South Academic Forum." For example: co-authoring and publishing DSI assessment reports for Brazil and Russia with scholars from these countries; introducing the DSI framework to relevant Brazilian government departments and academia through cooperation with institutions such as the "China-BRICS Artificial Intelligence Development and Cooperation Center"; integrating DSI concepts into sovereign AI and digital sovereignty strategy consulting provided to Ghana's Ministry of Information and local governments through the partner consulting firm Aether Strategies; and so on.

These preliminary practices indicate that DSI has the potential to become an effective bridge connecting academic research with policy practice and promoting solidarity and cooperation among Global South countries. The ultimate goal of this research is to hope that

DSI can develop into a knowledge tool and action guide that empowers Global South countries, helping countries gain greater voice and autonomy in the global digital governance landscape, and ultimately building a continuously evolving digital sovereignty dialogue, research, and collaboration ecosystem around this index that is jointly led by Global South countries.

Regarding how to promote the digital sovereignty independence movement of the Global South and strive for and strengthen the level of digital sovereignty independence and autonomy of Global South countries, the author proposes the following recommendations.

First, at the level of intergovernmental multilateral cooperation, discussions on digital sovereignty should be initiated on the BRICS platform to enhance the importance of digital sovereignty among BRICS countries and the current status of digital sovereignty in the Global South, promote multilateral dialogue and collaboration on the BRICS platform, jointly improve digital sovereignty standards and measurement systems, and jointly advocate for a new global digital governance order based on multilateralism, respecting the digital sovereignty of all countries, and promoting unity and cooperation. This year (2025), Brazil assumed the rotating presidency of BRICS and proposed six "priority work topics," including "encouraging inclusive and responsible AI governance for development." A recent article co-authored by the author and Amadeu has pointed out that digital sovereignty, especially independence and autonomy in digital infrastructure and data ownership, is a prerequisite for countries to independently own and govern artificial intelligence. Currently, the author is actively promoting discussions on digital sovereignty organized by the BRICS Civil Society Organizations Forum and striving to include the digital sovereignty topic in the agenda of this year's July BRICS Summit.

Second, at the level of industrial cooperation, Global South countries other than China should strengthen cooperation with Chinese ICT enterprises, gradually breaking free from the current status of heavy dependence on American large enterprises to provide digital infrastructure, and gradually enhancing the degree of autonomous control over digital infrastructure in their own countries. At the same time, in the fields of digital space governance and data ownership, Global South countries should be vigilant: the primary purpose of Chinese companies going overseas is profit, and they will not automatically and spontaneously advocate for the digital sovereignty of the partner country. Global South countries should use the indicator system of the Digital Sovereignty Index as a reference, formulate their own digital sovereignty strategies, and require Chinese ICT enterprises to comply with and assist in this strategy. The intergovernmental multilateral cooperation mechanism proposed in the first point can provide macro guidance for industrial cooperation.

Third, at the level of academic research, Global South countries, especially BRICS countries, should jointly participate in digital sovereignty-related research. There are mainly two academic research directions in this field: one is to conduct baseline assessments of the digital sovereignty status of various countries using the DSI framework, and form specific policy recommendations for enhancing digital sovereignty levels based on the current status; the second is to continue improving the Digital Sovereignty Index, strengthening the quantifiability and repeatability of the indicator system, including using artificial intelligence technologies such as large language models (LLMs) to convert large amounts of qualitatively described industry news and research reports into relatively quantifiable and horizontally comparable ratings, thus forming a relatively objective evaluation mechanism. Currently, the author is collaborating with researchers and policy participants in relevant fields from Brazil, Russia, South Africa, India, and China to jointly promote the development and application of the Digital Sovereignty Index. In the long term, the author expects to establish a continuous tracking and assessment mechanism for the Digital Sovereignty Index of Global South countries, and establish a dialogue and collaboration platform for Global South countries on digital sovereignty issues around this index.

China Digital Sovereignty Index Assessment Report

China has become the world's largest economy (by purchasing power parity). Over the past few decades, China has continuously developed its electronics and information industry, achieving remarkable results. China has reached relatively high levels in most indicators of the Digital Sovereignty Index and has become the country with the highest degree of digital sovereignty independence and autonomy outside the United States. It has demonstrated advanced thinking and practices that lead the world on the critical question of "how to make data value inclusive for the people," and is also making active efforts to advocate for and safeguard the digital sovereignty of Global South countries. China's experience and achievements in striving for digital sovereignty have important reference significance for other Global South countries. Below, the author will use the Digital Sovereignty Index measurement system to assess China's level of digital sovereignty. This assessment is based entirely on publicly released information.

China's Data Ownership Independence Status

1.1. Legislation on data ownership

Since 2016, China has successively formulated three framework laws related to data ownership protection: the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law. China's data protection-related legislation has largely drawn on the EU's GDPR, granting individuals rights such as the right to informed consent, the right to access and portability of personal information, the right to correction, the right to deletion, the right to restrict processing, and the right to object, all of which are highly similar to the GDPR. Beyond the series of rights protecting personal information, China's related legislation has also made institutional arrangements for the security assurance and orderly flow of large-scale data as a whole (which includes but is not limited to personal information), laying the foundation for fully releasing data value.

Within the framework of these three laws, China has formulated a series of laws and regulations guiding specific implementation. For example, the Cybersecurity Law made principled and framework provisions on the collection and protection of personal information by network products and services. Subsequently, the Cyberspace Administration of China (CAC) issued the "Provisions on the Management of Mobile Internet Application Information Services," specifically releasing corresponding guidance on personal information protection for mobile applications and mini-programs, and conducting a series of enforcement activities. As another example, the Personal Information Protection Law stipulates that enterprises involved in processing personal information should audit their activities of how they process personal information (i.e., "personal information protection compliance audit"). In response to this provision, in August 2023, the CAC released the "Measures for the Administration of Personal Information Protection Compliance Audits (Draft for Comments)," providing clear guidance for personal information processors on how to conduct personal information protection compliance audits.

China's Cyberspace Administration system consists of the Cyberspace Administration of China (CAC) and its branches in local governments. This system is the main enforcement body for network and data security supervision and network personal information protection. The Cyberspace Administration system has been quite active in internet governance. Taking just the first half of 2022 as an example, the national Cyberspace Administration system dealt with a total of 3,491 illegal network platforms, of which more than 400 were substantially penalized, and a number of network platforms with problems of illegal or improper collection and use of personal information were forced offline for rectification. The most famous case may be the ride-hailing platform DiDi (with a business model similar to Uber), which was fined 8.026 billion yuan (5% of the previous year's revenue) in July 2022 for long-term illegal collection or excessive collection of personal information, illegal processing of more than 60 billion pieces of multiple types of sensitive personal information, and refusing to fulfill regulatory requirements and maliciously evading supervision. This demonstrates China's determination and intensity in implementing related legislation. The relevant regulations on protection of minors on the internet and on algorithm recommendation management promulgated after DiDi's huge penalty were all quickly and effectively implemented.

In summary, in terms of data ownership, China has formed an overall legal framework and continues to improve laws and regulations guiding specific implementation within this framework. The strong enforcement system led by the Cyberspace Administration ensures that the continuously issued new regulations are implemented. On the indicator of "Legislation on data ownership," the author gives a rating of "Level 5: Independent."

Legislation on data ownership—
Level 5: Independent

1.2. Domestic data storage

The Cybersecurity Law stipulates that critical information infrastructure in important industries and fields such as public communications and information services, energy, transportation, water conservancy, finance, public services, and e-government, as well as other critical information infrastructure that may seriously endanger national security, national economy and people's livelihood, and public interest if damaged, loses function, or suffers data leakage, should store personal information and important data collected and generated in domestic operations within China's borders.

In February 2014, the Central Leading Group for Cyberspace Affairs was established, with the General Secretary of the Communist Party of China and President personally serving as the group leader. In the same year's "Two Sessions," "safeguarding network security" was written into the government work report for the first time. This is the historical background for the initiation of the Cybersecurity Law. It can be seen that the protection of critical information infrastructure and important data is considered from the perspective of national security.

On the other hand, China's independence and autonomy in digital infrastructure, especially in the cloud computing industry, is a prerequisite for data to be stored domestically. For example, the cloud service "Cloud on Guizhou" used by Apple iCloud in China to store data is a domestic cloud platform jointly built by the Guizhou provincial government and Alibaba Cloud, established in November 2014. In 2015, the State Council issued the "Opinions on Promoting Cloud Computing Innovation and Development and Cultivating New Formats of the Information Industry," further promoting the widespread penetration of cloud computing, especially domestic cloud platforms, in various industries. Multiple fields including government, finance, e-commerce, transportation, and healthcare have all launched application cases based on cloud computing, and enterprise cloud adoption has become an important means to accelerate digital transformation. The vast majority of data generated domestically is naturally stored on domestic cloud platforms.

In summary, China regards personal information and important data collected and generated in the operation of critical information infrastructure as part of national security and has clear legislation requiring that this data be stored within China's borders. Furthermore, the independent and autonomous cloud computing infrastructure makes domestic storage of domestic data a natural choice. On the indicator of "Domestic data storage," the author gives a rating of "Level 5: Independent."

Domestic data storage—Level 5: Independent

1.3. Protection of cross-border data transfers

The Cybersecurity Law stipulates that personal information and important data collected and generated in the domestic operations of critical information infrastructure in China, if they need to be provided abroad due to business needs, should undergo security assessments according to the measures formulated by the national Cyberspace Administration in conjunction with relevant departments of the State Council. The concept of "important data" is clarified in the form of national standards. The national standard "Data Security Technology - Data Classification and Grading Rules" (GB/T 43697-2024) issued in March 2024 lists 17 factors to consider for identifying important data, such as: data that directly affects territorial security and national unity, or reflects the basic situation of the country's natural resources, such as unpublished land, territorial waters, and airspace data; data that directly affects the market economic order, such as data supporting core business operations in industries and fields where critical information infrastructure is located or production in important economic fields. Various industries have more detailed national standards or industry standards to specifically stipulate the importance and security protection levels of various types of data, such as the industry standard "Financial Data Security - Data Security Grading Guide" (JR/T 0197-2020), which stipulates security grading rules for typical data of financial institutions.

Based on the provisions of the Cybersecurity Law, the CAC has successively issued the "Measures for Standard Contracts for Personal Information Exit" and the "Measures for Data Exit Security Assessment," clarifying specific methods for data exit management: if data processors need to provide personal information above a certain scale (100,000 people) abroad, they need to use standard contracts and file with provincial-level Cyberspace Administration departments; if they need to provide important data, sensitive personal information, and large-scale (more than 1 million people) personal information abroad, they must also undergo mandatory data exit security assessments. To guide and help data processors standardize and orderly report data exit security assessments and file personal information exit standard contracts, the CAC has compiled the "Data Exit Security Assessment Declaration Guide" and the "Personal Information Exit Standard Contract Filing Guide," explaining specific requirements for the methods, processes, and materials for reporting data exit security assessments and filing personal information exit standard contracts.

After the promulgation of the above laws and regulations, the Cyberspace Administration system conduct-

ed centralized baseline investigations of internet enterprises, critical information infrastructure operators, and foreign enterprises involving important data and large amounts of personal information. The ride-hailing platform DiDi mentioned earlier was severely punished and subsequently delisted from the New York Stock Exchange because it needed to provide massive amounts of personal information and important data to the U.S. Securities and Exchange Commission (SEC) and other regulatory agencies after going public on the New York Stock Exchange, and did not implement data exit security assessments and filings as required. Tesla CEO Musk also promised that "personal identity information of Chinese users will not cross borders, and important data will be exported after approval by the competent authorities."

It should be noted that the above legislative and enforcement actions do not mean that China opposes cross-border data flows. On the contrary, after securing data security and personal information protection with a series of laws and regulations, the CAC issued the "Provisions on Promoting and Regulating Cross-border Data Flows" in November 2023, clearly stating that "data collected and generated in activities such as international trade, cross-border transportation, academic cooperation, transnational production and manufacturing, and market marketing that is provided abroad and does not contain personal information or important data is exempt from reporting data exit security assessments, concluding personal information exit standard contracts, and obtaining personal information protection certification"; allowing free trade pilot zones to independently establish negative lists for data exit, "data processors in free trade pilot zones providing data outside the negative list abroad can be exempt from reporting data exit security assessments, concluding personal information exit standard contracts, and obtaining personal information protection certification." Only with strict data security protection can there be open cross-border data flows and data cooperation, rather than unidirectional data extraction.

In summary, China attaches great importance to the security and controllability of cross-border flows of important data and personal information, has adopted a series of legislative and enforcement measures to ensure data security and personal information protection, and on this basis encourages open cross-border data flows and data cooperation, achieving refined risk management and reflecting the principle of "lawful, orderly, and free flow of data," highlighting China's determination to advance high-level opening-up in the digital field. The author's evaluation of China on the indicator of "Protection of cross-border data transfers" is "Level 5: Independent."

Protection of cross-border data transfers—Level 5: Independent

1.4. Inclusion of data value for the public

Large amounts of data accumulated on internet platforms originally come from hundreds of millions of users, yet their value is monopolized by private internet enterprises and cannot benefit society as a whole. This problem has not had a good solution for a long time. The socialist market economy with public ownership as the main body and diverse forms of ownership developing together is China's basic economic system. Under this economic system, if data sourced from the public is managed as a public asset, it may be a feasible path to achieve the inclusion of data value for the public.

The Fourth Plenary Session of the 19th CPC Central Committee held in 2019 for the first time listed "data" as a production factor, alongside traditional production factors such as "labor, capital, land, knowledge, technology, and management." This is a major innovation in economic theory, the first time in more than a hundred years since Marshall in 1890 identified "entrepreneurial ability" (which contains multiple components such as knowledge, technology, organization, and management) as the fourth type of production factor beyond land (including natural resources), capital, and labor, that a new type of production factor has been proposed from the perspective of economic theory.

A series of policies issued subsequently began to promote the implementation of this theoretical innovation. The "Opinions on Building a More Perfect Market-oriented Allocation System and Mechanism for Production Factors" issued in 2020 proposed "accelerating the cultivation of data factor markets." The "14th Five-Year Plan and 2035 Vision Goals Outline" issued in 2021 proposed "establishing and improving data factor market rules" and "cultivating standardized data trading platforms and market entities, developing market operation systems such as data asset evaluation, registration and settlement, transaction matching, and dispute arbitration." The "Opinions on Building a Data Basic System to Better Play the Role of Data Factors"

issued in 2022 proposed "exploring a structural data property rights separation system… establishing a property rights operation mechanism with separate data resource holding rights, data processing and use rights, and data product operating rights."

Based on these policy directions, the "Interim Provisions on Accounting Treatment Related to Enterprise Data Resources" issued by the Ministry of Finance at the end of 2022 clarified specific accounting methods for data resources to be included in balance sheets (to be "on the books"), especially clarifying that "data resources held by enterprises in daily activities with the ultimate purpose of sale… should be recognized as inventory," fundamentally changing the long-standing situation where data could only be hidden in balance sheets as intangible assets, greatly expanding the space for data to be converted into economic value.

In 2024, several urban investment enterprises (i.e., state-owned enterprises of the "urban investment" type responsible for local infrastructure construction) achieved data asset capitalization. As state-owned enterprises, urban investment enterprises obtain data created by the public in the process of building and operating infrastructure. By putting data assets on the books, the value of data is actually transformed into the appreciation of state-owned assets, which is then realized for the benefit of all people through the management and deployment of the State-owned Assets Supervision and Administration Commission. Another case is the newly built "millennium city" Xiong'an New Area near Beijing, where all the data generated by the entire smart city is uniformly owned, uniformly managed, and uniformly operated by the state-owned enterprise China Xiong'an Group Digital City Technology Co., Ltd. Although technology companies such as Huawei, Tencent, and Alibaba participate in the construction of the digital city, they can only provide technology and equipment and cannot obtain data. It can be foreseen that in the future, when Xiong'an's data assets begin to generate economic value, it will naturally form the appreciation of state-owned assets, thus benefiting all people. In this closed loop of data taken from the people, used for the people, and benefiting all people, state-owned enterprises owning and operating public data is a key.

In summary, China has initially established the economic theory of treating data as a new type of production factor, formulated a series of policies to build data factor markets and improve data value distribution systems, and demonstrated a clear orientation toward public ownership of public data and inclusion of data value for the public. Currently, this field is still in the early exploration stage, and it is expected to take several years or even a decade to form a relatively mature system. The author's evaluation of China on the indicator of "Inclusion of data value for the public" is "Level 3: Developing."

Inclusion of data value for the public—Level 3: Developing

China's Digital Infrastructure Independence Status

China's ICT (Information and Communication Technology) market totaled $592.13 billion in 2023, or $419.4 per capita. Due to its large population, China's per capita ICT market size among the BRICS founding five countries is higher than Russia and India, but lower than South Africa and Brazil; however, in terms of total volume, China's ICT market size is one-third higher than the sum of the other four countries. The huge market size has given China the space for independent industrial development.

On the other hand, China has been committed to developing an independent and autonomous electronics, information, and communications industry since the Mao era, and successive generations of national leaders have consistently implemented this strategy. After decades of accumulation, China has basically mastered autonomy in all aspects of digital infrastructure, including hardware, software, and information security.

2.1. Independence of foundational hardware

The Digital Sovereignty Index mainly examines the level of independence and autonomy in three types of foundational hardware: chips, servers, and storage devices.

Semiconductor chip production is mainly divided

into three major processes: design, manufacturing, and packaging and testing, and requires upstream semiconductor equipment and materials as support. Among these, the chip manufacturing process has high technological barriers and requires large capital investment, leading to extremely high industry concentration. Currently, the industry presents a competitive landscape dominated by TSMC. Integrated circuits are China's largest import commodity category, especially high-end chips such as processors and controllers, which have a relatively high degree of dependence on imports. Due to well-known geopolitical factors, Taiwan's chip manufacturing industry is highly controlled by the United States. In the past few years, the United States has continuously escalated its suppression of China's semiconductor industry, restricting China's access to high-end chips or the ability to produce these chips. This pressure has caused certain difficulties for Chinese communications companies that use large numbers of high-end chips (such as Huawei), while also transforming into motivation for China to continuously develop an independent and autonomous semiconductor industry. In 2022, China's mainland chip manufacturing capacity accounted for 26% of the global total, already ranking second globally—the first is China's Taiwan region, accounting for 46% of global capacity.

Lithography machines are core equipment used for chip manufacturing and are also the "chokepoint" key link in the United States' restriction of China's access to high-end chips. In January 2023, the United States, Japan, and the Netherlands reached an agreement to ban the export to China of some of the most advanced semiconductor manufacturing equipment, including extreme ultraviolet (EUV) and deep ultraviolet (DUV) lithography machines produced by the Dutch manufacturer ASML. Despite severe import restrictions, Huawei still used 7-nanometer chips produced by Shanghai-based SMIC to release the Mate 60 Pro high-end phone during U.S. Commerce Secretary Raimondo's visit to China in 2023. It is reported that SMIC has already set up a completely new 5-nanometer semiconductor chip production line in Shanghai using existing lithography machines, and is expected to begin mass production of new-generation chips designed by Huawei as early as 2024. On the other hand, the "Catalog of Major Technical Equipment (First Set) for Popularization and Application (2024 Edition)" issued by the Ministry of Industry and Information Technology in 2024 lists argon fluoride lithography machines with a resolution ≤65nm, indicating that domestically produced lithography machines can already meet almost all chip manufacturing scenarios except smartphones.

China's server manufacturing has a high degree of domestication. In 2022, China's server market sold about 4.22 million units in total, with the highest market share held by the state-controlled Inspur Information (28.1%), followed by H3C, a Chinese-foreign joint venture with Chinese controlling interest (17.2%). Dell, the foreign company with the highest market share, only accounts for 5.1% of the market.

Enterprise-level storage is also a highly domesticated market. In China's enterprise-level storage market in 2023, six leading Chinese companies including Huawei (30.6%), Inspur (11.0%), H3C (10.5%), Hikvision (6.8%), Lenovo (5.9%), and Sugon (5.9%) occupied more than 70% of the market share, while Dell, the foreign company with the highest market share, only accounts for 4% of the market.

In summary, China currently has the capability to independently produce most foundational hardware, but still has considerable dependence on imports (including imports from Taiwan) in chips, especially high-end chips manufacturing, and still has obvious vulnerability to U.S. technology blockades. However, China has been working hard to make up for shortcomings in this area and has made significant progress. It is expected that within a few years, China will have the capability to independently produce the most advanced lithography machines. Currently, the author's evaluation of China on the indicator of "Independence of foundational hardware" is "Level 4: Competent."

Independence of foundational hardware—Level 4: Competent

2.2. Independence of foundational software

The Digital Sovereignty Index mainly examines the level of independence and autonomy in four types of foundational software: operating systems, databases, middleware, and cloud platforms.

On Chinese people's desktop computers, Microsoft Windows still occupies an absolute dominant position, with a market share as high as 84%. Apple OS X, ranking second, is about 8%. Domestic operating systems

have less than 3 million annual installations and annual sales revenue of less than 2-billion-yuan, accounting for less than 4% of China's domestic market. Domestic operating systems have not yet formed a market mechanism-driven, effective, stable, and sustained user demand.

In July 2021, the Ministry of Industry and Information Technology and other six departments issued the "Guiding Opinions on Accelerating the Cultivation and Development of High-Quality Manufacturing Enterprises," proposing to increase efforts to tackle key core technologies and products in fields such as foundational software. The "14th Five-Year Plan for Digital Economy Development" issued in January 2022 requires focusing on improving the supply level of foundational software and strengthening the self-sufficiency guarantee capability of key products. Under the guidance of these policies, the IT application innovation (Xinchuang, meaning domestic substitution of foundational and key information technology) industry has become a highly focused track, and some domestic operating systems (such as Kylin and UOS) have gradually matured and gained certain market applications.

Server-side operating systems are mainly open-source Linux, and the difficulty of domestication is relatively low, and the progress of domestication is also relatively fast. According to data released by Huawei, the company's developed openEuler has reached a 36.8% market share in China's server operating system new market, ranking first. Based on calculations by an investment institution, the future market capacity of China's Xinchuang operating system market can reach more than 20 billion yuan per year, and domestic manufacturers still have considerable development space. In addition, Huawei's HarmonyOS system has also occupied a considerable share in the smartphone operating system market. In the first quarter of 2024, HarmonyOS's market share reached 17%, surpassing Apple's iOS (16%) to become the second-largest operating system in China's smartphone market (the first is Android).

China's database market reached 23.643 billion yuan in 2022, an increase of 10.2% over 2021, with database software accounting for about 86.4%, with a market size of about 20.432 billion yuan. The vendor that achieved the first market share in on-premises database products is still the U.S. company Oracle. However, since 2008, local internet companies such as Alibaba have already started the trend of "removing IOE" (i.e., replacing IBM minicomputers, Oracle databases, and EMC storage devices with open-source architectures and general products on the server side). Since 2019, databases for China's financial core systems have begun to be domesticated, and to date, 95 domestic database products have been successfully put into production in core systems of multiple financial industries such as banking, securities, and insurance. Gartner predicted in its 2022 "Database China Market Guide Report" that by 2025, overseas vendors in China's analytical database market will only have 30% remaining, and overseas vendors in the transactional database market will only have about 50% remaining.

China's middleware industry currently presents the characteristics of numerous participants and low market concentration. In the field of foundational middleware, foreign companies dominate with an 85.6% market share; in the field of broad middleware, foreign companies have a 60% market share. Overall, the leading tier of China's middleware industry mainly consists of U.S. companies such as IBM, Oracle, and Microsoft, which have obvious advantages in technology accumulation, global brand influence, and server field supporting support; following closely are domestic companies with strong financial strength, financing capabilities, and development potential, which are divided into two major fields: in the foundational middleware field, such as TongTech, Jindie, Primeton, Kingdee Apusic, and BaoLand, and in the broad middleware field, such as Alibaba Cloud and Tencent Cloud. Under the influence of the Xinchuang policy, the market share of domestic middleware may continue to increase.

China's cloud computing market reached 616.5 billion yuan in 2023, a year-on-year increase of 35.5%, significantly higher than the global growth rate. It is expected that by 2024, the cloud computing market size will reach 837.8 billion yuan, a year-on-year increase of 35.9%. Due to constraints related to domestic data storage and cross-border flow policies, U.S. companies have significantly insufficient motivation to conduct cloud computing business in China, and China's cloud computing market is mainly occupied by local companies. According to IDC data, leading companies in China's IaaS and PaaS market share in 2022 include Alibaba Cloud (31.9%), Huawei Cloud (12.1%), China Telecom e-Cloud (10.3%), and Tencent Cloud (9.9%), followed by AWS from the United States (8.6%).

In summary, China still has considerable dependence on U.S. companies in foundational software such as operating systems, databases, and middleware, and has a relatively high degree of independence and autonomy in the cloud computing field. The Chinese government is promoting Xinchuang domestication from the perspective of geopolitics and national security. Leading Chinese ICT companies (such as Huawei) and internet companies (such as Alibaba) are also gradually replacing software imported from the United States with software they have developed themselves, which includes both considerations of supply chain security and purely economic considerations. With the joint efforts of all parties, China's domestic foundational software already has the capability to fully replace imported software and is expected to gain greater development space in the future. The author's evaluation of China on the indicator of "Independence of foundational software" is "Level 4: Competent."

Independence of foundational software—Level 4: Competent

2.3. Independence of application software

The Digital Sovereignty Index mainly examines a country's application software autonomy level from three perspectives: office software, general software, and industry software.

In 1988, Qiu Bojun, who graduated from the National University of Defense Technology of the Chinese People's Liberation Army, developed WPS, which was the world's first Chinese word processing software, released earlier than Microsoft Office. By 2022, Microsoft Office and WPS Office had coverage rates of 81.5% and 68.7% respectively in China's domestic Windows platform market; WPS's monthly active users (MAU) on mobile devices reached 336 million, more than 10 times that of Microsoft Office. It can be said that in the Chinese market, WPS is comparable to Microsoft Office on the PC side and has surpassed Microsoft Office on the mobile side.

In the field of general software, China's huge market has cultivated a large number of competitive enterprises. For example, in ERP (Enterprise Resource Planning) software, Chinese local enterprises dominate. According to Gartner data, leading manufacturers such as Yonyou, Inspur, and Kingdee rank at the forefront, with a combined market share of 72%, far higher than foreign companies such as SAP and Oracle. However, in the high-end market, domestic manufacturers are at a relative disadvantage. With the rapid increase in digitalization and the major development of local internet companies, China's general software market presents increasingly high entry barriers, and few foreign companies can succeed in this market.

In the field of industry software, Chinese companies overall present the situation of "strong in management software, weak in engineering software; many low-end software, few high-end software." Foreign software giants occupy more than 80% of the domestic industrial software market from design, manufacturing to service, and control core technologies of industrial software such as simulation design, analysis tools, enterprise management, and advanced control. More than 150 mainstream commonly used industrial software in various fields internationally, covering research and development design, production control, testing and verification and other links, are almost all provided by foreign companies, and the software is closed and not open-source. In particular, research and development design industrial software is China's industrial software shortcoming, with a low domestication rate. According to data from the "China Industrial Software Industry White Paper (2020)," China's research and development design industrial software domestication rate is only 5%, and 95% of research and development design industrial software depends on imports. Current domestic research and development design industrial software is mostly applied in fields with relatively simple industrial mechanisms and low industry complexity. Industrial software has high technical requirements, complex knowledge systems, long R&D cycles, and large capital investments, making it difficult for local manufacturers to catch up later. This type of software may still become a chokepoint for the West to "strangle" China.

In summary, China's software market with an annual scale of more than 10 trillion yuan (about 1.4 trillion U.S. dollars) has cultivated a large number of domestic software companies. However, some high-end industry software (such as industrial software) still has relatively high barriers, with a low degree of domestication and high dependence on foreign manufacturers. The author's evaluation of China on the indicator of "Independence of application software" is "Level 4: Competent."

Independence of application software—Level 4: Competent

2.4. Independence of information security

Since Snowden disclosed the "PRISM" program in 2013, China has begun to pay attention to the United States' implementation of large-scale surveillance and cyber-attacks on other countries through its "offensive cyber deterrence strategy"—according to an analysis by Global Times, this strategy was introduced during the Obama period, became the core pillar of U.S. cybersecurity strategy during the Trump period, and further expanded the scope of deterrence during the Biden period. The Beijing-based 360 Digital Security Group summarized that the United States, using its first-mover advantage in the internet field, has formed seven major capabilities for creating cybersecurity threats globally, including using submarine cables to monitor global data flows, using global internet root servers and CA certificates to interfere with the fair development of the internet in various countries, using operating systems and internet services to obtain sensitive data, using open-source communities to implement supply chain attacks, using standards and protocols to deploy the security of key products, using the global common vulnerability disclosure standard and operating agencies to obtain security vulnerabilities first, and using cyber weapons to attack the infrastructure of other countries.

China's Cybersecurity Law issued in 2016 requires network service operators to implement security protection measures in accordance with the network security level protection (referred to as "MLPS") regulations, and the Ministry of Public Security has also issued a series of network security level protection policy documents organically connected with laws and regulations, such as the "Guiding Opinions on Implementing the Network Security Level Protection System and Critical Information Infrastructure Security Protection System" (Public Network Security [2020] No. 1960) and the "Guiding Opinions on Implementing Key Measures for Network Security Protection and In-Depth Implementation of the Network Security Level Protection System" (Public Network Security [2022] No. 1058), thereby giving birth to a nascent network security market. In 2022, China's network security market size was about 63.3 billion yuan (about 9 billion U.S. dollars). As of the first half of 2023, a total of 3,984 companies nationwide were engaged in network security business, of which 26 network security companies were publicly listed. At the same time, in response to the U.S. cyber deterrence strategy, China highly values the independence and autonomy of the information security industry, and foreign companies (especially U.S. companies) have almost completely withdrawn from this industry.

Currently, China's information security system is entirely passive and defensive. Combining the seven major capabilities of the United States to create cybersecurity threats, for attack methods that exploit the underlying mechanisms of the internet, such as submarine cable monitoring, root server attacks, and open-source supply chain attacks, China currently lacks effective countermeasures. For example, the Log4J security vulnerability that occurred in November 2021 caused security threats to 2.5-3 billion devices worldwide and 44% of corporate networks. As another example, Durov, the founder of the instant messaging tool Telegram, pointed out that the U.S. government only needs to add a backdoor to software through an open-source software library. These cases all illustrate the extreme importance and extreme fragility of the open-source supply chain. However, China currently does not have a systematic software supply chain security guarantee mechanism, and only a few companies such as Huawei have carried out open-source and third-party software governance practices internally. If at some point China really needs to face a comprehensive cyber attack from the United States, it is still an unknown how much protection the existing defensive information security system can provide.

In summary, under the pressure of U.S. cybersecurity threats, China has developed a basically independent and autonomous, defensive information security system; however, for some attack methods controlled by the United States that exploit the underlying mechanisms of the internet, China currently still lacks countermeasures. The author's evaluation of China on the indicator of "Independence of information security" is "Level 4: Competent."

Independence of information security—Level 4: Competent

China's Digital Governance Independence Status

3.1. Legislative capacity for digital affairs

In addition to the legislation on network security and data protection already introduced earlier, China's legislative work in the field of digital economy is also developing rapidly. In particular, for some common challenges in the digital economy that the whole world faces, China is leading the way in related legislation.

Regulation of information algorithm recommendation is one example. Many researchers have pointed out that algorithm recommendation can easily form "information cocoons," causing social division and even being used to manipulate public opinion and influence politics. In response to this world-class problem, the CAC and other departments issued the "Provisions on the Management of Algorithm Recommendation in Internet Information Services" in 2022, proposing the overall requirement of "promoting algorithm application toward good and upward," and making clear provisions on security requirements, review and evaluation mechanisms, rule transparency and interpretability, user rights protection, supervision and management mechanisms and other issues for algorithm recommendation services, making it the world's first regulation specifically regulating network information algorithm recommendation.

Another world-class problem in the digital economy is the protection of workers' rights in the platform economy environment. Because platforms claim to only be responsible for matching supply and demand information and are not employers of workers, workers' rights are not guaranteed and working conditions continue to deteriorate. Many people call this employment form the "gig economy." The Ministry of Human Resources and Social Security issued in 2024 a series of regulations for the protection of workers in new employment forms under the platform economy, such as the "Guidance on the Protection of Rest and Labor Remuneration Rights of Workers in New Employment Forms," "Guidance on the Publication of Labor Rules for Workers in New Employment Forms," and "Service Guide for the Protection of Rights of Workers in New Employment Forms," implementing the main responsibility of internet platform employment, and making clear provisions on issues of urgent concern to workers providing services through internet platforms (such as working hours and rest rights, labor remuneration, labor dispute resolution mechanisms, and trade union rights), fundamentally solving the problem of internet platforms evading responsibility and workers' rights having no place to be implemented.

In response to the common problem of large internet platforms using traffic advantages to create monopolies, the Anti-Monopoly Committee of the State Council issued the "Anti-Monopoly Guidelines for the Platform Economy Field" in 2021, prohibiting monopolistic behaviors such as monopoly agreements, abuse of market dominance, concentration of business operators, and abuse of administrative power to exclude or restrict competition.

In response to the potential risks of artificial intelligence, the "Interim Measures for the Management of Generative Artificial Intelligence Services" implemented by the CAC in August 2023 put forward requirements for AIGC service providers in terms of content security, prohibition of discrimination, fair competition, and data quality, and connected with existing regulations such as information content supervision, personal information protection, intellectual property rights, unfair competition, science and technology ethics, generated content identification, security assessment, and algorithm filing, together with the "Science and Technology Ethics Review Measures (Trial)" issued by the Ministry of Science and Technology and other departments in September 2023, jointly constructing the preliminary framework of China's AIGC governance. In addition, at the level of standard documents, the National Information Security Standardization Technical Committee issued the "Network Security Standard Practice Guide - Methods for Identifying Content Generated by Generative Artificial Intelligence Services" in August 2023, aiming to implement the relevant requirements for generative content identification in the above "Interim Measures"; in October, it issued the "Basic Security Requirements for Generative Artificial Intelligence Services (Draft for Comments)," refining the basic security requirements for generative artificial intelligence services, including corpus security, model security, security measures, and security assessment.

In short, facing the objective reality of continuous technological innovation and model innovation in the digital age, China adopts an agile governance and

small-incision legislation path, starting from multiple levels such as laws, regulations, policies, and standards in parallel, quickly establishing a governance system adapted to technological development, with legislation efficiency and effectiveness leading the world. The author's evaluation of China on the indicator of "Legislative capacity for digital affairs" is "Level 5: Independent."

Legislative capacity for digital affairs—Level 5: Independent

3.2. Enforcement capacity for digital affairs

For the supervision and governance of domestic digital affairs, China has established an enforcement system led by the CAC with coordination from various departments. Requirements for enterprises are usually standards first, with enterprise self-inspection and rectification as the main focus, and for enterprises that still do not rectify within the deadline and continue to violate laws and regulations, severe penalties are imposed, especially showing no mercy to industry-leading large enterprises, which has played a very good deterrent role for the entire industry.

For example, in April 2021, the State Administration for Market Regulation determined that e-commerce giant Alibaba violated the Anti-Monopoly Law by abusing its dominant position in the domestic online retail platform service market, prohibiting or restricting merchants on the platform from opening stores on other platforms, restricting market competition, infringing on the legitimate rights and interests of merchants on the platform, and harming consumer interests, and fined Alibaba 18.228 billion yuan (about 2.78 billion U.S. dollars). In October 2021, the State Administration for Market Regulation punished Meituan for abusing its market dominance in the online food delivery platform service market in accordance with the Anti-Monopoly Law, ordered Meituan to immediately stop illegal activities and return the "exclusive cooperation guarantee deposit," and imposed a fine of 3.442 billion yuan (about 490 million U.S. dollars), with the fine amount being 3% of the company's 2020 revenue. In 2021, the State Administration for Market Regulation executed a total of 89 internet anti-monopoly penalties, with almost all Chinese internet technology giants on the penalty list.

This round of heavy penalties has clearly established the authority of law in the internet industry. Facing subsequent legislation (such as the "Provisions on the Management of Algorithm Recommendation in Internet Information Services" issued in 2022, the "Provisions on the Management of Internet Pop-up Information Push Services" issued in 2022, the "Interim Measures for the Management of Generative Artificial Intelligence Services" and the "Regulations on the Protection of Minors on the Internet" issued in 2023, and the "Provisions on the Governance of Cyber Violence Information" issued in 2024, etc.), internet companies can generally implement them decisively and thoroughly, thus forming a good interaction between regulatory units and enterprises. In addition, the CAC has opened convenient reporting channels to facilitate the general public to report illegal and harmful information. In 2023, various reporting channels received and processed a total of 206 million reports from netizens, playing a very important supervisory role in promoting the construction of a good online ecology.

In summary, the strict enforcement by the CAC and market supervision and other regulatory agencies ensures that China's rapidly updated digital space legislative governance system is effectively implemented. Although Chinese regulatory agencies do not yet have long-arm jurisdiction over internet service providers located outside the country's borders, given that the vast majority of Chinese people mainly use domestic services in their daily internet use, the Chinese government's regulatory and enforcement capabilities are sufficient to protect their safety and rights. The author's evaluation of China on the indicator of "Enforcement capacity for digital affairs" is "Level 5: Independent."

Enforcement capacity for digital affairs—Level 5: Independent

3.3. Leadership in international digital technology rules

The technological development direction and route of the ICT industry are largely influenced by Standards Development Organizations (SDOs). The Atlantic Council's report regards how many voting seats a country has in several important SDOs as an important criterion for a country to dominate technology rule-making and occupy a leading technological position, and points out that U.S. hegemony in this field is facing challenges from China.

In fact, although China's position in various important SDOs has improved, the gap with the United States is still huge. In important standardization organizations in the electronics, information, and communications technology fields such as W3C, The Open Group, SNIA, IEEE, and OMA, the United States occupies more than 40% of voting seats. In standardization organizations such as OSGi, OGF, IEC Secretariat, and ITU, the United States has less than 30% of the seats, but is also significantly higher than China. Only in 3GPP in the field of mobile communications technology and the Car Connectivity Consortium (CCC) in the field of intelligent vehicles does China's voting seats exceed those of the United States.

Organization	Total Members	US Members	US %	Chinese Members	Chinese %	apanese Members	Japanese %
W3C	359	152	42.34%	30	8.36%	34	9.47%
The Open Group	900	452	50.22%	16	1.78%	16	1.78%
SNIA	18	11	61.11%	3	16.67%	2	11.11%
OSGI	14	4	28.57%	1	7.14%	1	7.14%
OGF	14	4	28.57%	1	7.14%	1	7.14%
IEEE	25	15	60.00%	6	24.00%	1	4.00%
IEC Secretariat	197	27	13.71%	15	7.61%	24	12.18%
ITU	126	23	18.25%	0	7.94%	19	15.08%
3GPP	836	102	12.20%	186	22.25%	48	5.74%
OMA	28	12	42.86%	1	3.57%	0	0.00%
CCC	93	16	17.20%	17	18.28%	17	18.28%

Distribution of voting seats in several important SDOs

Overall, China's influence in international SDOs (measured by voting seats) is roughly equivalent to Japan's, able to contribute its efforts to the formulation of international digital technology rules, but far from reaching the level of being able to challenge U.S. hegemony. The author's evaluation of China on the indicator of "Leadership in international digital technology rules" is "Level 3: Developing."

Leadership in international digital technology rules—Level 3: Developing

3.4. Leadership in international digital behavior rules

The "Overall Layout Plan for Digital China Construction" issued in 2023 proposed: "Expand the space for international cooperation in the digital field, actively participate in digital field cooperation platforms under multilateral frameworks such as the United Nations, World Trade Organization (WTO), Group of Twenty (G20), Asia-Pacific Economic Cooperation (APEC), BRICS countries, and Shanghai Cooperation Organization (SCO), build new platforms for open cooperation in the digital field with high quality, and actively participate in the construction of international rules related to cross-border data flows." In addition, China has actively applied to join international digital trade agreements such as DEPA and CPTPP, actively participated in global digital trade international cooperation, improved the international rules system, and proposed China's solutions for developing digital trade.

As mentioned earlier, China and the United States have major differences on many aspects of international digital rules. For example, on the issue of computing facility location and cross-border data flows: the United States believes that there should be no restrictions on where data is stored or on cross-border data flows (the result of which is that the vast majority of data from around the world flows into the United States); while China, based on its actual situation, believes that important data should be stored within its own borders and that cross-border data flows must prioritize safeguarding national security and interests. These differences are reflected in specific trade agreements. The "U.S.-Japan Digital Trade Agreement," DEPA, and CPTPP tend toward the U.S. view, stipulating that "public policy exception measures cannot constitute… disguised restrictions on trade"; while the China-led RCEP introduces exception clauses for national security and makes hard provisions that contracting parties cannot raise objections to related measures.

In the opinion "China's Position on Issues Related to Global Digital Governance" submitted by China's Ministry of Foreign Affairs to the United Nations regarding the formulation of a "Global Digital Compact" in 2024, it pointed out that "two markets, two sets of standards, and two supply chains are emerging in the network and digital field." On prominent issues in digital development and global digital governance, China has proposed four basic principles: adhering to unity and cooperation, focusing on promoting development, promoting fairness and justice, and promoting effective governance. On the basis of these four basic principles, China has proposed several specific recommendations, including: countries should respect the sovereignty, jurisdiction, and security management rights over data of other countries; oppose interfering in other countries' internal affairs and challenging other countries' judicial sovereignty in the name of safeguarding online human rights; countries have the right to implement protection, management, and guidance on the dissemination of network information within their territories, etc. These recommendations are clearly different from the current U.S.-led international digital rules and reflect the actual demands of the vast number of Global

South countries.

In summary, China has envisioned a fairer global digital governance new order that is more beneficial to the Global South, and has begun to attempt to practice this vision in the construction of international digital rules. However, China's current scope of influence on international digital rules is still limited. The author's evaluation of China on the indicator of "Leadership in international digital behavior rules" is "Level 3: Developing."

Leadership in international digital behavior rules—Level 3: Developing

China's Digital Capability Independence Status

4.1. Cutting-edge technology research and development

According to the World Intellectual Property Organization (WIPO)'s patent technology classification, Category I "Electrical Engineering" (including 5 subcategories: 1. Electrical machinery, apparatus, energy; 2. Audio and video technology; 3. Telecommunications; 4. Information technology; 5. Semiconductors) can basically be regarded as digital industry-related technologies. The number of patents a country obtains under this major category can also serve as an indirect indicator of that country's scientific research and innovation capability in the digitalization field. In 2022, of the more than 610,000 international patents granted under Category I, China accounted for 273,000 (45% of the total), ranking first in the world, more than double that of the United States (112,000), which ranks second. According to OECD data, from 2017 to 2020, ICT-related patents accounted for 52.2% of all patents in China, a proportion that is also the highest among countries in the world (as a comparison, this proportion in the United States is 36.1%, in India 27.9%, and in Brazil 8.8%). These two data points indicate that China has a solid foundation and huge scale of scientific research and innovation in the field of digital technology.

At the same time, China also faces some practical challenges in cutting-edge scientific research in the field of digital technology. First, the intensity of R&D investment is still low compared to the United States. Of the total R&D investment of the world's 2,500 companies with the largest R&D investment in 2022, 40% came from the United States, and the proportion from China was 18%, with a significant gap compared to the United States. In addition, China's dependence on imports in fields such as core equipment, key basic materials, and high-end chips is still relatively high, and there are situations where key core technologies are controlled by others in many fields such as lithography machines, chips, operating systems, core industrial software, and core algorithms. Taking all factors into consideration, the author's evaluation of China on the indicator of "Cutting-edge technology research and development" is "Level 4: Competent."

Cutting-edge technology research and development—Level 4: Competent

4.2. Talent cultivation in universities

According to OECD data, in 2020, the total number of university graduates in Science, Technology, Engineering, and Mathematics (STEM) disciplines in China was 3.57 million, accounting for 41% of the total number of all university graduates, both of which are the highest in the world. According to data published by People's Daily, China's current annual number of STEM discipline graduates has exceeded 5 million. A Georgetown University study believes that by 2025, the number of doctoral graduates in STEM disciplines in China will be close to twice that of the United States. Although not all STEM discipline graduates will engage in digitalization-related work, it is undeniable that the emphasis on STEM disciplines has laid a deep talent reserve for China's digitalization process.

In April 2024, the "Action Plan for Accelerating the Cultivation of Digital Talent to Support the Development of the Digital Economy (2024-2026)" issued by the Ministry of Human Resources and Social Security proposed "combining digital talent needs, deepening new engineering research and practice in the digital field, strengthening the construction of digital field-related disciplines and majors in higher education institutions, and increasing the cultivation of interdisciplinary talents. Giving full play to the role of vocational colleges, promoting the upgrading and digital transformation of vocational education majors, and adding a number of

new majors in the digital field. Promoting the construction of digital technology-related courses, textbooks and tutorials, and teaching teams. Deepening the integration of industry, academia, and research, supporting universities, research institutes, and enterprises to jointly cultivate composite digital talents." As the country attaches importance to the digital economy, China's education system is likely to continue to play the role of a global (not just China's) digital talent cultivation engine for a long time in the future. The author's evaluation of China on the indicator of "Talent cultivation in universities" is "Level 5: Independent."

Talent cultivation in universities—Level 5: Independent

4.3. Industry engineering capabilities

In 2021, the total number of people engaged in digitalization-related work such as information and communications, software, and information technology services in China was 5.192 million, and this number was only about 180,000 in 2000. One of the important factors contributing to the industry's rapid development over more than 20 years is the country's support for this industry. The "Several Policies to Encourage the Development of the Software Industry and Integrated Circuit Industry" (State Council Document [2000] No. 18, referred to as "Document 18" in the industry) issued in 2000 is a landmark policy. In 2001, the country established the National Leading Group for Informatization Work, with then-Premier Zhu Rongji personally serving as the group leader and proposing the policy of "emphasizing e-government construction." This policy drove the major development of domestic ICT companies. Around 2010, several U.S. internet giants successively withdrew from China, leaving development space for a number of Chinese internet companies such as Baidu, Alibaba, and Tencent. Today, China's industry engineering and technical capabilities are quite mature, forming a complete and effective transformation path from scientific research to products. A shortcoming of China's digital industry is that the industry's summary of its engineering methods is still lacking, and most companies in the industry are still trying to use methodologies originating from the United States (such as CMMI, Agile, etc.) to standardize their engineering and technical activities, and often feel that these methodologies are not well adapted to China's actual situation in many ways. Nevertheless, China's digital industry's engineering and technical capabilities are still strong and possess complete independence and autonomy. The author's evaluation of the indicator of "Industry engineering capabilities" is "Level 5: Independent."

Industry engineering capabilities—Level 5: Independent

4.4. Coordination of digital technology with national development strategies

China's computer science and technology undertaking was born in the "12-Year Science Plan" (the "Long-term Plan for Science and Technology Development from 1956 to 1967," abbreviated as "12-Year Science Plan") formulated in 1956. At that time, China, which had just defeated the U.S. invaders on the Korean battlefield, was fully committed to socialist construction. Qian Xuesen, a missile and aerospace technology expert who returned to China from the United States, firmly promoted the inclusion of computer technology in the national science plan, especially listing the development of computers, semiconductors, radio electronics, automation, and remote manipulation technology as "emergency measures" in the "12-Year Science Plan." Subsequently, the Chinese Academy of Sciences established the Institute of Computing Technology, and universities such as Tsinghua University and the Military Engineering Institute of the Chinese People's Liberation Army established computer science departments, laying the first cornerstone of China's information technology. During this stage, the main purpose of China's development of information technology was military and aerospace automatic control, with the aim of mastering advanced strategic deterrence capabilities under the premise of being unable to obtain support from the United States or the Soviet Union, and it was also used for civilian computing tasks such as meteorology, dams, and transportation.

In the 1980s, China, which had entered the era of reform and opening-up, began to pay attention to the forefront of international information technology development. Jiang Zemin, then Minister of Electronics Industry, led a delegation to visit the United States and Canada in 1983, inspecting 34 companies and research units, and also visiting the 37th International Military Electronics and Communications Equipment Exhibition held by the United States and the European Community. In the inspection report, Jiang Zemin wrote: "The widespread application of electronic technology has greatly improved the production efficiency and

work efficiency of the two countries, the United States and Canada, and has become a powerful driving force for economic development." At the same time, Jiang Zemin also pointed out the industry trend that "communication technology is combined with computer technology and is rapidly developing in the direction of digitization." In 1984, Jiang Zemin proposed at the National Electronics Industry Bureau Chief Work Conference the development task of "by 2000, China's electronics industry total output value will triple compared to 1980, and the main products and production technology will reach the level of advanced industrial countries in the late 1980s and early 1990s of the 20th century, with some technologies reaching the world's advanced level at that time." Under Jiang's leadership, China's electronics industry achieved great development during this period, laying the industrial foundation for the later development of the information industry and digitalization industry. Document 18 in 2000 was a continuation of this development task and also reflected Jiang's consistent attention to the development of information technology while in national leadership positions.

In 2007, then-General Secretary Hu Jintao proposed at the 38th collective study session of the Political Bureau of the CPC Central Committee to "make the internet a new way to disseminate advanced socialist culture, a new platform for public cultural services, and a new space for people's healthy spiritual and cultural life," thereby opening the curtain on China's internet supervision and governance. Looking back at the role the internet played in events such as the Eastern European color revolutions and the Arab Spring that occurred during the same period, it can be seen that China's emphasis on digital space sovereignty and national security is reasonable and effective.

In recent years, as its digital technology and industrial capabilities have gradually entered the world's advanced ranks, China has also increasingly focused on the relationship between the digital economy and the real economy. In 2017, General Secretary Xi Jinping proposed at the second collective study session of the Political Bureau of the CPC Central Committee to "implement the national big data strategy, accelerate the improvement of digital infrastructure, promote the integration and open sharing of data resources, ensure data security, accelerate the construction of Digital China, and better serve China's economic and social development and the improvement of people's lives," and specifically required "promoting the integrated development of the real economy and the digital economy, promoting the deep integration of the internet, big data, and artificial intelligence with the real economy, continuing to do a good job on the major article of deep integration of informatization and industrialization, and promoting manufacturing to accelerate development toward digitization, networking, and intelligence." Starting from the fundamental question of "whether it can promote the development of the real economy and whether it can improve people's lives," China has prudently treated technical concepts hyped by Silicon Valley such as blockchain, NFT, and the metaverse, vigorously promoted 5G and industrial internet, and also adopted an attitude of equal emphasis on development and supervision for large language models and artificial intelligence technology. Judging from the current effects, although China still lags behind the United States in many areas of digital technology, the driving effect of digital technology on the real economy and the improvement effect on people's lives are better than those of the United States.

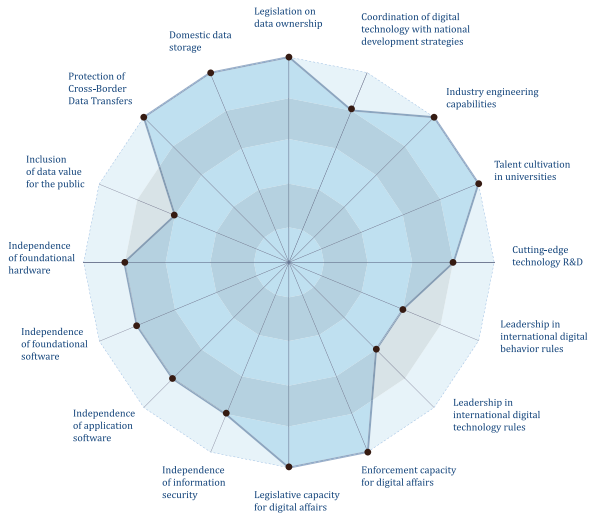
But at the same time, it should be noted that China's current level of export of technology and governance experience in the digital field is still limited and does not match the international influence needed to build a community with a shared future for mankind and practice the three initiatives (Global Development Initiative, Global Security Initiative, and Global Civilization Initiative). In the coming period, how to share and promote China's digital technology and governance experience to Global South countries will be an important task for the coordination of the digital field with national development strategies.

In summary, China has adopted different policies to develop the information industry in its various historical periods. These policies both serve the political and economic needs of the time and maintain the consistent goal of seeking scientific and technological and industrial independence and autonomy and serving the people over a span of nearly 70 years. However, how to relate digital technology to the vision of building a community with a shared future for mankind is not yet clear. The author's evaluation of China on the indicator of "Coordination of digital technology with national development strategies" is "Level 4: Competent."

Coordination of digital technology with national development strategies—Level 4: Competent

Conclusion and Outlook

In summary, China's Digital Sovereignty Index assessment results are shown in the figure below:



China's Digital Sovereignty Index Assessment Results

Looking back to the 1980s, China's nascent civilian ICT industry was not even at the level of Brazil. But China has always adhered to an independent and autonomous strategy, using a "whole-nation system" to tackle cutting-edge scientific and technological challenges, supporting the development of local enterprises, and cultivating large numbers of specialized technical talents. After more than thirty years of accumulation and continuous development, China's digitalization industry has been able to basically possess independent and autonomous capabilities in most fields. Although there is still dependence on the global supply chain, especially on advanced European and American technology, China already has the confidence to face the suppression and sanctions unilaterally imposed by the United States.

At the China-Africa Cooperation Forum Beijing Summit in September 2024, President Xi Jinping proposed the grand vision of "leading Global South modernization with China-Africa modernization." Digitalization is an important component of modernization. Controlling digital sovereignty, developing the digital economy, and achieving inclusive data value for the people are inherent obligations of the Global South's realization of modernization. From the Digital Sovereignty Index assessment results, China's international influence in the digital field is still lacking, especially the leadership capacity in international digital technology rules and international digital behavior rules still has considerable development space. In the future, China needs to continue to promote its achievements and experience in digital technology and digital governance with the Global South as the main target, participate more actively in and lead the construction of international digital rules, and play a leading role in the process of building a fairer and more just new order for global digital governance.

Brazil's Digital Sovereignty Index Assessment Report

This article was published in Liinc em Revista, Brazil. Citation information:

SILVEIRA, Sergio Amadeu; XIONG Jeff. dice de soberania digital: o caso do Brasil. *In: Liinc em Revista*, v. 21, n. 01, e7451. Disponível em: https://revista.ibict.br/liinc/article/view/7451. Acesso em: 04 jul. 2025.

As an important country in the Global South, the largest nation in Latin America, and a significant member of the BRICS organization, Brazil's progress in various aspects has attracted the attention of numerous countries in the Global South. In recent years, the Brazilian government has also repeatedly proposed strengthening the country's digital sovereignty development. However, the assessment finds that Brazil's overall digital sovereignty level is still relatively weak, as the country has neither managed to reduce its dependence on foreign countries and their companies (mainly U.S. companies), nor has it formulated transitional policies aimed at strengthening autonomy and independent control. Brazil still has a long way to go in developing national digital capabilities and achieving digital sovereignty. Below, the authors will use the Digital Sovereignty Index, a metric measurement system, to assess Brazil's digital sovereignty level. This assessment is entirely based on publicly available information.

Current State of Brazil's Data Ownership Independence

1.1. Legislation on data ownership

The Brazilian Constitution stipulates the right to protection of personal data (including personal data in digital media) (Constitutional Amendment No. 115 of 2022, Incluído pela Emenda Constitucional nº 115, de 2022) and explicitly addresses the protection of personal data and the supervision of personal data processing activities. The General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, abbreviated as LGPD), passed in September 2020, is Brazil's first comprehensive law on data protection, providing a comprehensive legal framework for companies and individuals to collect, use, process, and store data. Beyond the LGPD, Brazil's protection of personal data is also scattered across other laws and regulations. For example, Federal Law No. 12965/2014 and its Decree No. 8771/16 (collectively known as the "Brazilian Internet Framework") impose requirements on service providers, network and application providers regarding the processing of personal data and other obligations, and clearly define the relevant rights of internet users.

Compared to the EU's GDPR, the LGPD and its detailed regulations are less stringent and more lenient regarding requirements for the financial sector. The LGPD introduced specific provisions regarding credit protection and fraud prevention that differ from the GDPR approach. According to the LGPD, financial institutions can process and share credit information without prior consent from data subjects, enabling banks and credit reporting agencies to conduct risk analysis and establish credit profiles more quickly. By prioritizing assessment of repayment capacity and reducing credit to those unable to repay, if algorithms are poorly designed or perpetuate historical biases, the LGPD cannot actually prevent exclusion or discrimination against vulnerable groups. Additionally, fraud prevention work protected by the LGPD requires large-scale data collection and monitoring, including behavioral and biometric data, which severely affects privacy. The collection of this data encourages intrusive practices in the system, leading to continuous data breach incidents within these institutions. Furthermore, the standard contract stipulated in the draft "International Transfer of Personal Data Regulations" (which details the cross-border data transfer mechanisms stipulated by the LGPD) released in August 2023 does not limit excessive data requests like EU standard contractual clauses. The maximum fine for violating the LGPD is 2% of the company's annual revenue in Brazil and does not exceed 50 million reais (approximately 8.9 million USD or 63.36 million RMB), which is incomparable to the severity of EU GDPR regulators being able to impose fines of up to 20 million euros or 4% of global annual turnover (whichever is higher) on violating organizations.

Articles 52, 53, and 54 of the LGPD related to administrative penalties officially came into effect only in August 2021. Its enforcement agency, the National Data Protection Authority (Autoridade Nacional de Proteção de Dados, abbreviated as ANPD), although established in December 2018, has not taken many actions over the past few years. Its staffing has been limited, with still few technical, auditing, and administrative personnel, reflecting the policy orientation of then-President Jair Bolsonaro. Currently, the ANPD's main work is still refining the relevant regulations of the LGPD, and has not yet implemented any penalties related to the LGPD, so enforcement effectiveness remains to be observed.

In summary, Brazil has promulgated the main legislation around data ownership, the LGPD, which is less severe compared to the EU's GDPR, and its actual enforcement effectiveness remains to be observed. On the indicator of "legislation on data ownership," the authors give a rating of "3 - Developing."

Legislation on data ownership — 3 - Developing

1.2. Domestic data storage

According to the LGPD, regardless of where the headquarters of the enterprise operating digital business is located or where data processing takes place, as long as the processed data belongs to Brazilian citizens or individuals within Brazil's territory, or if the personal data being processed was collected within Brazil's territory, the LGPD applies. However, neither the LGPD nor other relevant laws explicitly specify whether data generated within Brazil's territory or by Brazilian citizens in the process of using services needs to be stored locally within Brazil's territory.

Brazil's digital ecosystem heavily relies on U.S. tech giants, who have different attitudes toward "data lo-

calization storage." Before the EU promulgated the GDPR, Microsoft had suggested allowing its customers to choose to store data in nearby locations outside the United States; whereas Google has consistently opposed the concept of data localization storage. With the promulgation of the GDPR and the popularization of cloud computing, tech giants have deployed data centers around the world. However, in the absence of clear legal requirements, where data is stored in which data center mainly depends on factors such as access speed and retrieval efficiency, determined by the companies' own algorithms, and does not guarantee that data generated domestically is necessarily stored within national borders.

Countries such as Russia and China have clear requirements for data localization storage. In 2023, Google was fined 15 million rubles (approximately 165,000 USD) by a Moscow court for violating data localization storage requirements. In contrast, domestic storage of data has not yet been put on the agenda in Brazil. On the indicator of "domestic data storage," the authors give a rating of "1 - Initial."

Domestic data storage — 1 - Initial

1.3. Protection of cross-border data transfers

The LGPD requires that personal data be adequately protected during cross-border transfers—the concept of "adequate protection" is defined as: transfer to countries or international organizations pre-certified by ANPD, or the organization controlling the data can adequately ensure compliance with the principles stipulated by the LGPD, data subject rights, and data protection systems, including specific contractual clauses for cross-border transfers, standard contractual clauses, global corporate norms, regularly published certifications or codes of conduct, etc. In August 2023, ANPD issued Resolution CD/ANPD No. 19, approving the "International Transfer of Personal Data Regulations" (Regulamento de Transferências Internacionais de Dados) and the "Standard Contractual Clauses Template" (Pessoais e do modelo de Cláusulas-Padrão Contratuais).

ANPD will determine a list of countries or regions with adequate protection levels to allow free flow of personal data between Brazil and these countries or regions. The "Draft Regulations" make clear that ANPD will prioritize evaluating the data protection levels of foreign countries or international organizations that guarantee reciprocal treatment to Brazil. This evaluation work is one of ANPD's key priorities in 2025.

Overall, Brazil's restrictions on cross-border data flows are extremely lenient, and the evaluation of data protection levels of other countries and international organizations has not yet been initiated. This reflects both the political influence of the financial sector and big tech companies in Brazil, as well as the fragility of democratic and left-wing forces in recognizing technological issues as fundamental aspects of national development. Therefore, data, as an important input to the information economy and the current artificial intelligence paradigm, remains in a secondary position on the agenda of major government departments. The authors' evaluation of Brazil on the indicator of "protection of cross-border data transfers" is "1 - Initial."

Protection of cross-border data transfers — 1 - Initial

1.4. Inclusion of data value for the public

Data is a fundamental input to the digital economy. It is the raw material for current artificial intelligence. Data can be defined as capital. In political economy, capital refers to resources, assets, or goods used to produce other goods and services. From data and algorithmic systems, new data, goods, and services are generated.

As leaders in the digital economy, both China and the United States have deliberate legislative initiatives to make data value inclusive to the public, and China's actions are more advanced than the United States. In 2019, California Governor Gavin Newsom proposed to let the state's citizens share a "data dividend," but this concept has not translated into any actual action. In the same year, the Fourth Plenary Session of the 19th Central Committee of the Communist Party of China listed data as a new type of production factor, and subsequently, multiple state-owned data trading markets were established under the leadership of local governments, improving the data assetization mechanism. In 2024, a group of transportation-related state-owned enterprises listed the data assets they owned on their balance sheets, achieving appreciation of state-owned assets.

Meanwhile, Brazil has not had in-depth discussions on data monetization and the distribution of capital derived from data. Data is exported from the country as if it has no high value. The next section of this article will show that Brazil's digital infrastructure independence is relatively low, making it difficult to control data generated domestically, with the vast majority of data still controlled by U.S. tech giant companies. Under the objective conditions of not yet reclaiming data ownership, the issue of data value distribution has not yet become a focus of attention in the country's academic, policy, and industrial circles. The authors' evaluation of Brazil on the indicator of "inclusion of data value for the public" is "1 - Initial."

Inclusion of data value for the public — 1 - Initial

Current State of Brazil's Digital Infrastructure Independence

Brazil's ICT (Information and Communication Technology) market totaled $96.66 billion in 2022, or $449 per capita. This per capita market volume ranks second among the BRICS five countries (only lower than South Africa), slightly higher than China ($419.4). However, like South Africa, Brazil's population is far less than China or India, with a smaller total market volume, making it difficult to form a scaled autonomous industry. Its ICT industry is concentrated in outsourcing, system implementation, and services, with weak autonomous research and development capabilities.

2.1. Independence of foundational hardware

The Digital Sovereignty Index mainly examines the independent autonomy level of three types of foundational hardware: chips, servers, and storage devices.

Brazil has a huge consumer market for personal computers, smartphones, and other digital products, but the plan to develop its domestic semiconductor industry launched in 2002 did not meet expectations. The state-owned semiconductor institution CEITEC, established in 2002, closed in 2020. As of 2020, Brazil's chip revenue accounted for only 3.2% of the global market. Furthermore, Brazil has no front-end wafer fabs. Although the country has several integrated circuit design companies, the number is far below initial expectations. In short, Brazil's semiconductor industry development has been hampered by factors such as lack of funding and policy support. Currently, Brazil has temporarily abandoned the idea of building wafer fabs, but continues to explore markets with lower capital requirements, such as integrated circuit design, storage modules (such as USB drives, solid-state drives, etc.), and packaging. This also means that the country's main chip supply will continue to depend entirely on foundry production by wafer fabs in other countries for the foreseeable future.

The top three manufacturers in Brazil's domestic server market are the U.S. companies HP and Dell, and China's Lenovo. Among the top ten manufacturers, there is only one Brazilian company, Positivo Tecnologia S/A. The country has a certain server autonomous production capacity, but dependence on foreign supply is still high.

The top six manufacturers (and market share) in Brazil's domestic storage device market are Dell (29.7%), HP (9.9%), Huawei (9%), NetApp (8.3%), Pure Storage (6%), and Hitachi (4.4%). Not a single Brazilian company enters this list.

In summary, Brazil's current level of foundational hardware independence is relatively low. The government and industry have some awareness of this situation, but have not yet taken proactive actions to make up the gap. The authors' evaluation of Brazil on the indicator of "independence of foundational hardware" is "2 - Aware."

Independence of foundational hardware — 2 - Aware

2.2. Independence of foundational software

The Digital Sovereignty Index mainly examines the independent autonomy level of four types of foundational software: operating systems, databases, middleware, and cloud platforms.

President Lula in his first term (beginning in 2003) advocated the use of free software and instructed government ministries and state-owned enterprises to gradually transition from expensive operating systems produced by companies like Microsoft to free operating systems like Linux. The government also launched

a project called "PC Conectado" (Connected Computer), providing computers priced within 1,200 reais (approximately $500) to the country's citizens, using the operating system Insigne Linux based on Fedora Linux—this system was developed by a Brazilian company. In 2008, Insigne Linux once had more than 1.5 million users. Insigne Linux stopped being maintained after releasing version 5.0.1 in 2010. According to the authors' knowledge, operating systems currently used domestically in Brazil are almost all produced by foreign manufacturers. Other free software projects under development, such as Portal do Software Público, were gradually interrupted and abandoned after President Dilma Rousseff was removed by coup in 2016.

In the 1980s, COBRA (now BB Tecnologia e Serviço S/A) created a Brazilian operating system called SOX for microcomputers manufactured in Brazil, using Motorola's 32-bit processor architecture. This project faced strong opposition from the United States and Brazilian media, whose interests aligned with those of large companies like IBM. The demise of this project can also be partially attributed to a series of errors made by the military in executing the country's so-called "computer policy."

According to the authors' knowledge, Brazil has no well-known autonomous domestic database products.

In the early 21st century, Brazil developed the digital television middleware solution Ginga, created by PUC-RJ and the Federal University of Paraíba. Although the technology was recognized by the International Telecommunication Union, it encountered resistance from all segments of the digital television market, and continuous changes in the hardware and software industries made Ginga increasingly irrelevant in the era of rapid digitalization and internet development.

An important reference for evaluating Brazil's cloud infrastructure and services is the "2023 ICT Enterprise Survey," which found that 55% of Brazilian companies outsource their IT infrastructure, and among companies with more than 250 employees, this number rises to 75%. The same research report also points out that 48% of Brazilian companies store files or databases in the cloud. Research also shows that companies have contracted email (53%), office software (34%), security software (46%), financial or accounting software (49%), and application development, testing, or deployment platforms (24%) to cloud services.

In 2019, the renowned journal "Exame" disclosed that according to Hostmapper data, the Brazilian company Locaweb, founded in 1998, hosted approximately 20% of Brazilian internet content on its servers. Locaweb focuses on website hosting, internet services, and cloud computing. A 2011 study by International Data Corporation (IDC) showed that Locaweb was the market leader in this field in Brazil and Latin America. However, recent information shows that Locaweb has lost its advantage in competition with international tech giants. In fact, the latest data indicates that Brazil's cloud infrastructure (IaaS) market is divided among three international giants: Amazon AWS, Microsoft, and Huawei.

According to data from the Observatório da Educação Vigiada (Observatory of Monitored Education), the two big tech companies Google and Microsoft currently provide email and data storage for 154 federal and state public universities in Brazil. Google provides digital mailboxes for 114 universities, accounting for 74.03% of these institutions. Microsoft provides services for 26 universities, accounting for 16.8% of the total. This means that researchers, students, and teachers at the country's top universities rely on the infrastructure of two major U.S. digital oligopolies (CRUZ et al.). During President Bolsonaro's administration, Rede Nacional de Pesquisa (National Research Network) was one of the main promoters of the policy of entrusting email and data services to Google and Microsoft.

In summary, Brazil's level of foundational software independence is very low, and the government and industry have not shown concern about this issue. Developments in the foundational software and cloud supply fields indicate that technological progress has been achieved without adequate participation of local developers. Conversely, there has been a decline in the development of leadership and independent initiatives. The rise of neoliberalism has severely affected independent technology development policies, especially in the government sector. The authors' evaluation of Brazil on the indicator of "independence of foundational software" is "1 - Initial."

Independence of foundational software — 1 - Initial

2.3. Independence of application software

The Digital Sovereignty Index mainly examines a country's application software independence level from three perspectives: office software, general software, and industry software.

Brazil's software industry totaled $21.25 billion in production in 2022, of which the "domestic software production" portion accounted for 13.1%, with a production value of $2.79 billion (by comparison, the "foreign software development" portion had a production value of $8.88 billion, accounting for 41.8%).

A research report released by the Brazilian Software Companies Association (ABES) on 2023 shows that Brazil's software and services market reached $26.863 billion, with the software market at $15.260 billion (accounting for 56.8%) and the services market at $11.603 billion (accounting for 43.2%) (ABES, 2024, p. 9). These figures place Brazil 11th in global rankings, accounting for 1.5% of the total market in 2023 (p. 8). ABES survey results show that software developed in Brazil that year only accounted for 24.8% of software in use (including exports), meaning less than a quarter of software is locally produced (p. 9).

The ABES research also emphasizes that there are approximately 37,602 companies in the domestic market engaged in software development and production, distribution, and service provision. Among them, 9,062 companies focus on software development and production, and 92.4% of companies can be classified as micro and small enterprises, meaning they employ no more than 99 people (p. 5).

In Brazil's software market, application development accounts for 51.7% of total activities, development environments account for 25.5%, infrastructure and security account for 21.3%, and local production for export accounts for 1.5%. When analyzing the end use of software and services, ABES research shows that the three main segments are services and telecommunications (25.9%), finance (25.6%), and industry (18.9%) (ABES, p. 11).

According to the definition of Brazil's Central Bank, fintech companies are enterprises that seek innovation and new business models in financial markets through the use of technology[2]. These companies extensively use software and mobile applications. According to a 2022 study by the Inter-American Development Bank (IDB)[3], in 2021, 31% of fintech companies in Latin America were headquartered in Brazil. According to data provided by the Brazilian Financial and Capital Markets Association (ANBIMA) based on the "2023 Global Fintech Outlook" survey, Brazil has 869 fintech companies (including 623 companies established locally), leading in the Latin American region and ranking seventh globally.

With the continuous development of applications based on generative artificial intelligence, dependence on cloud service providers is also increasing. Brazil's lack of deep learning infrastructure and frameworks is likely to deepen the country's dependence on large enterprises in software development.

Within Brazil's smaller-scale domestic software market, there is limited space for large-scale product research and development. However, overall, the number of enterprises and talents entering this industry is on an upward trend. The authors' evaluation of Brazil on the indicator of "independence of application software" is "2 - Aware."

Independence of application software — 2 - Aware

2.4. Independence of information security

Brazil began formulating a national cyber defense strategy in the early 21st century, established its first national cyber defense theory in 2014, and established a Joint Operations Command Center in 2016. These developments occurred during the presidencies of Lula and his successor Rousseff. An important reason driving these developments was that both the 2014 World Cup and 2016 Olympics were subjected to cyber attacks. Brazil's cyber defense capabilities are generally considered the best in Latin America, having provided cyber defense assistance to neighboring countries on multiple occasions during major regional events.

The Brazilian government has issued a series of decrees providing guidelines for cybersecurity and critical infrastructure. For example, Decree No. 9573/2018 defines the "National Critical Infrastructure Security Policy," and Decree No. 10569/2020 defines the "National Critical Infrastructure Security Strategy." However, it is worth noting that strategies and plans for

protecting critical infrastructure are currently only guidelines and have not been fully implemented. Currently, these decrees can be regarded as "soft" normative guidance documents—they cannot be enforced, nor can they penalize non-compliance. Although there are long-term plans to formulate mandatory rules and specific measures, these plans have not yet been implemented.

The National Cybersecurity Strategy (E-cyber) approved in 2020 is also soft law. Although E-cyber is not legally binding, it is an important tool that helps the government plan to improve the security and resilience of critical infrastructure and national public services.

In summary, Brazil has clear awareness of information security independence issues and has begun implementing a series of legislative and administrative measures. However, limited by insufficient autonomy in software and hardware infrastructure, Brazil's ability to control information security remains limited, and the implementation pace of relevant legislation is also slow. Furthermore, Brazil's deep dependence on basic software, applications, models, and infrastructure owned by large foreign companies raises doubts about the actual effectiveness and independence of Brazil's cybersecurity. The authors' evaluation of Brazil on the indicator of "independence of information security" is "3 - Developing."

Independence of information security — 3 - Developing

Current State of Brazil's Digital Governance Independence

3.1. Legislative capacity for digital affairs

Brazil was one of the earliest countries in the world to adopt the internet and established the Brazilian Internet Steering Committee (CGI.br), becoming an international benchmark in the Western world. However, the expansion of information networks, digital technologies, and digitalization occurred during a period when neoliberal theory was in vogue. Therefore, most Brazilian legislators and public administrators embraced privatization and underinvested in technology development. State-owned information technology and data processing companies, such as Serpro, Prodesp, Prodam, and Procergs, neither modernized nor readjusted their missions to keep pace with rapid technological changes and evolving business models. Since the late 1990s, the country has fallen into a deadlock: neoliberal administrators attempt to discredit and dissolve these state-owned IT enterprises with the aim of privatizing them; while nationalist-leaning politicians try to preserve these enterprises but lack sufficient political support and innovative strategies to realize their potential. As a result, the purchasing power of the Brazilian government is increasingly used to pay for solutions provided by large U.S. tech companies.

Despite lacking coherent digital technology development policies, Brazil played a key role in internet regulation by promulgating the Marco Civil da Internet (Internet Civil Framework), which consolidated important principles such as net neutrality, a set of privacy guarantees, and stable rules for the country's internet service providers, content providers, and digital network users. The law was passed by the Brazilian Parliament in 2013, when Edward Snowden exposed a global surveillance program orchestrated by the U.S. National Security Agency (NSA) that directly used U.S. tech companies as operators[6]. President Dilma Rousseff signed the Marco Civil Act into law in 2014. Although several telecommunications companies resisted this legislation, fearing it would strengthen net neutrality, the coalition of left-wing and liberal democratic forces ultimately demonstrated Brazil's legislative capacity on technological issues, contrary to the interests of large companies.

Nevertheless, the Marco Civil Act did not address the regulation of new digital enterprises that emerged in 2004 (such as online social networks and social media platforms) that mediate personal interactions. In an era where the digital economy increasingly depends on data, the law also had no intention of protecting data. Despite opposition from domestic and foreign banks and financial capital, the Brazilian Parliament passed a law of groundbreaking significance for citizenship, society, and the Brazilian economy: Law No. 13709 promulgated on August 14, 2018, the General Data Protection Law (LGPD), which stipulates rules for the collection, storage, sharing, and processing of personal data.

To discuss Brazil's digital independence, one cannot ignore the historical context in which these technologies were generated and applied. In particular, one must recognize the rise of far-right forces who are almost completely aligned with U.S. interests, the so-called entreguismo—combined with radical neoliberal policies. A country's legislative capacity in digital affairs largely depends on the balance of domestic political forces. In July 2020, Senator Alessandro Vieira proposed Bill No. 2630—"Brazilian Internet Freedom, Responsibility and Transparency Law," commonly referred to as the "fake news bill." After receiving Senate approval, the bill entered the Chamber of Deputies for further debate. After multiple public hearings, the bill's rapporteur, Representative Orlando Silva, proposed a version that made multiple requirements for digital platforms, including obligations to fact-check misleading posts, remove hateful or clearly illegal content, submit transparency reports, and inform individuals of reasons for post deletion or blocking, among other measures.

In April 2024, when the bill was ready for a vote in the Chamber of Deputies in Brasilia, it faced strong opposition from big tech companies. Google published a statement on its homepage claiming that "the fake news bill will increase confusion between true and false for Brazilians." Additionally, Google cooperated with Meta, dispatching lobbyists to pressure legislators and mobilizing influencers—who receive financial support through these platforms—to attack and undermine this bill aimed at regulating certain behaviors of digital platforms.

Far-right legislators, cooperating with a group called "Centrão," joined forces with big tech companies to prevent a vote on Bill No. 2630. Under intense lobbying by this alliance of extremists and U.S. companies, Chamber of Deputies President Arthur Lira—who has connections to Centrão—blocked the bill and announced the formation of a new Chamber of Deputies committee to draft an alternative proposal for regulating social network services. This decision demonstrates that big tech companies have the ability to intervene in any vote that might threaten their interests, thereby undermining the national sovereignty of legislative power.

To be even more cautious, big tech companies have also actively worked to weaken and dilute Brazil's regulation of artificial intelligence (AI). By promoting the questionable argument that regulating AI would stifle innovation, they gained the support of the National Confederation of Industry (CNI). As AI regulations advanced in Europe and other countries, the Brazilian Senate approved Bill No. 2338/2023 in December 2024[9]. Following Brazil's legislative procedures, the bill was then submitted to the Chamber of Deputies. Provisions initially proposed by civil society requiring reliable risk reports were weakened, but still allow unconstrained use of AI-driven facial recognition.

Broader legislation governing digital affairs (such as constraints on recommendation algorithms, special requirements for youth protection, constraints on artificial intelligence, etc.) has not yet emerged in Brazil.

In summary, Brazil is strengthening digital affairs legislation in key areas and has achieved significant progress. However, the political landscape is characterized by intense debates with far-right factions that support the interests of U.S. digital oligopolies. The authors' evaluation of Brazil on the indicator of "legislative capacity for digital affairs" is "3 - Developing."

Legislative capacity for digital affairs — 3 - Developing

3.2. Enforcement capacity for digital affairs

In recent years, Brazil has been working to enhance its capabilities in combating cybercrime. The Federal Police established a department in 2022 specifically to respond to the most complex cyber threats. However, according to the latest "Cyber Defense Index" released by MIT Technology Review, Brazil still lags behind many countries in cybersecurity policy, ranking second to last among 20 major countries.

The ANPD (National Data Protection Authority), the implementing unit for the LGPD, has been dedicated to formulating implementation rules related to the LGPD since its establishment. ANPD recently announced work themes and priorities for 2024 and 2025, determining work objectives, monitoring parameters, and expected dates for regulations to be issued. The first batch of implementation rules to be detailed covers areas such as data subject rights, processing of minor data, artificial intelligence, and data scraping.

Brazil's judiciary, particularly the Federal Supreme Court (STF), has played a key role in enforcing the Con-

stitution and national laws when faced with false information and the power held by digital oligopolies—especially large U.S. tech companies headquartered in the United States. In a dispute with the former Twitter platform (now "X"), the STF ordered the blocking of the microblogging service in Brazil. This decision was triggered by the refusal of X CEO Elon Musk to comply with Brazilian court orders, leading to the continued presence of content related to crimes, denialism, and support for the coup associated with the attempted coup on January 8, 2023. To undermine Brazil's judiciary, Musk decided to close X's office in Brazil.

The far-right American entrepreneur did this with the aim of preventing the implementation of Brazilian law and discrediting the judiciary. However, access to X was effectively blocked, and Brazilian authorities also launched investigations into Musk's other businesses in the country. Within just a few days after the blockage, as a large number of users left the X platform, Musk backed down and reopened X's office in Brazil. However, with Donald Trump's victory in the United States and Musk's subsequent appointment as a government official, he may once again challenge Brazil's ability to uphold its laws. In this effort, he is likely to receive support from Mark Zuckerberg and Meta Group, as well as other big tech companies, which are expected to adopt similar practices.

Overall, even under tense and turbulent international circumstances, Brazil has still demonstrated enforcement capacity in digital affairs. The authors' evaluation of Brazil on the indicator of "enforcement capacity for digital affairs" is "3 - Developing."

Enforcement capacity for digital affairs — 3 - Developing

3.3. Leadership in international digital technology rules

The direction and roadmap of technology development in the ICT industry are largely influenced by international standards development organizations (SDOs). A report by the Atlantic Council views the number of voting seats a country holds in several important SDOs as an important criterion for a country's leadership in technology rule-making and technological leadership, pointing out that U.S. hegemony in this area is facing challenges from China.

One manifestation of Brazil's ICT industry's overall weak R&D capabilities is the relatively few voting seats in SDOs. For example, among the 359 voting member organizations of W3C, which sets standards for the World Wide Web (WWW), only one is from Brazil: the Brazilian Network Information Center (NIC). Among the 4,135 voting "Participation Members" (P-Members) of the International Electrotechnical Commission (IEC), the world's oldest international standards organization responsible for international standardization in electrical engineering and electronic engineering, only 46 are from Brazil, accounting for only 1.1%, lower than countries like Iran and South Africa.

Additionally, Brazil has no voting representatives in several important SDOs, including the Standards Committee of the IEEE Standards Association, ITU platinum and gold members, 3GPP (the main standards organization in mobile communication technology), OMA (the main standards organization in mobile telephony), and Car Connectivity Consortium (the main standards organization in the smart vehicle field). From this data, it can be seen that Brazil's participation in the formulation of international digital technology standards is still in its initial stages.

Based on these indicators, the authors' evaluation of Brazil on the indicator of "leadership in international digital technology rules" is "2 - Aware."

Leadership in international digital technology rules — 2 - Aware

3.4. Leadership in international digital behavior rules

Due to relatively weak digital infrastructure and autonomous R&D capabilities, Brazil generally lacks leadership in the formulation of international digital behavior rules. However, some signs indicate that the country is actively participating in and influencing rule-making in this area. For example, the G20's Digital Economy Working Group (DEWG) is working with multiple governments to build a set of trustworthy and inclusive global Digital Public Infrastructure (DPI), particularly to address the long-standing digital divide faced by countries in the Global South—the concept of DPI was proposed last year when India held the G20 presidency. During its G20 presidency, Brazil actively promoted DPI discussions on topics such as digital identity and national data sharing, and will promote collaborative

cooperation within Latin America and the Caribbean at the ministerial meeting of the Digital Government Network of Latin America and the Caribbean (Red GEALC) in the second half of this year. Related outcomes are expected to be announced at this year's G20 summit. From this case, it can be considered that the Brazilian government is actively trying to participate in the formulation of rules for international digital behavior and digital interoperability. Therefore, the authors' evaluation of Brazil on the indicator of "leadership in international digital behavior rules" is "2 - Aware."

Leadership in international digital behavior rules — 2 - Aware

Current State of Brazil's Digital Capability Independence

4.1. Cutting-edge technology research and development

According to the World Intellectual Property Organization (WIPO) patent technology classification, Category I "Electrical Engineering" (including 5 subcategories: 1. Electrical machinery, apparatus, and electrical energy; 2. Audio-visual technology; 3. Electronic communication; 4. Information technology; 5. Semiconductors) can basically be equated with digitalization industry-related technologies. The number of patents a country obtains under this major category can also serve as an indirect indicator of that country's technological R&D innovation capabilities in the digitalization field. In 2022, among the more than 610,000 international patents granted under Category I, Brazil had only 275, ranking 27th in the world. According to OECD data, from 2017 to 2020, ICT-related patents accounted for only 8.8% of all patents in Brazil (by comparison, this proportion was 27.9% in India, 36.1% in the United States, and 52.2% in China). These two data points show that Brazil's technological R&D innovation capabilities in the digitalization field are still weak. The authors' evaluation of Brazil on the indicator of "cutting-edge technology research and development" is "2 - Aware."

Cutting-edge technology research and development — 2 - Aware

4.2. Talent cultivation in universities

In 2020, Brazil had a total of 238,000 university graduates in science, technology, engineering, and mathematics (STEM) disciplines, higher than Mexico, France, and Germany. STEM discipline graduates accounted for 17% of total university graduates. On the other hand, a considerable proportion of Brazil's STEM discipline graduates may go to work in Europe and America, leading to a certain degree of brain drain. The authors' evaluation of Brazil on the indicator of "talent cultivation in universities" is "3 - Developing."

Talent cultivation in universities — 3 - Developing

4.3. Industry engineering capabilities

In 2021, Brazil had approximately 1.9 million ICT practitioners nationwide, an increase of approximately 200,000 from 2020. OECD research suggests that Brazil's R&D expenditure in the ICT field remains insufficient. The main support for R&D in the ICT field—the Informatics Law—has helped increase manufacturing production and employment, but the policy does not seem to have achieved the goal of stimulating innovation and improving productivity. Other initiatives to enhance digital industry engineering and technical capabilities, such as the National Council for Scientific and Technological Development (Conselho Nacional de Desenvolvimento Científico e Tecnológico, CNPq) "Advanced Manufacturing Technology Grants and Scholarships," as well as projects from the Brazilian National Development Bank (BNDES), the Brazilian National Research Foundation (FINEP), and the Brazilian Company for Industrial Research and Innovation (Empresa Brasileira de Pesquisa e Inovação Industrial, EMBRAPII) "Internet of Things or Advanced Manufacturing Projects," although they have played an incentive role,

remain limited in quantity and funding scale. The "Brazilian Artificial Intelligence Strategy" approved in 2024 has made progress compared to its predecessor, but it has not proposed a coherent set of initiatives or identified priority timelines. The authors' evaluation of Brazil on the indicator of "industry engineering capabilities" is "3 - Developing."

Industry engineering capabilities — 3 - Developing

4.4. Coordination of digital technology with national development strategies

As early as the military government era in the 1970s, Brazil adopted a series of policies to protect and promote its domestic information industry: first, controlling the import of computers and related components; second, government procurement prioritized domestic suppliers; third, supporting relevant enterprises in the information industry chain and providing preferential policies, etc. From these three aspects, as early as the 1970s-1980s, Brazil clearly saw the importance of the information industry for national development and the enormous potential of the future information industry. The information industry policies of this period also played a positive role in promoting the development of related national industries. From the mid-1970s to the early 1980s, Brazil's information industry became one of Brazil's fastest-growing industrial sectors, with an annual growth rate of 37%. COBRA, a Brazilian national computer company founded in 1974, became the world's second-largest computer manufacturer by 1984, second only to IBM. By 1985, 35 out of every 1,000 people in Brazil owned a microcomputer, second only to the United States and Japan. Throughout the 1980s, Brazil's top ten domestic manufacturers occupied about 80% of the national computer market, dominated the domestic microcomputer industry, and "cloned" U.S. operating systems.

However, in 1985, President Sarney canceled previous information industry policies, and Brazil was also hit by a trade war launched by the United States in the information industry field. After 1991, new information industry policy laws were passed, and Brazil entered a period of information industry trade liberalization, gradually abandoning the development strategy of an autonomous and controllable semiconductor industry system. This also created the current situation where Brazil's overall digital technology capabilities are relatively weak. COBRA was acquired by Banco do Brasil and renamed "BB Tecnologia e Serviços" (BBTS) in 2013, essentially becoming the information technology service department of Banco do Brasil.

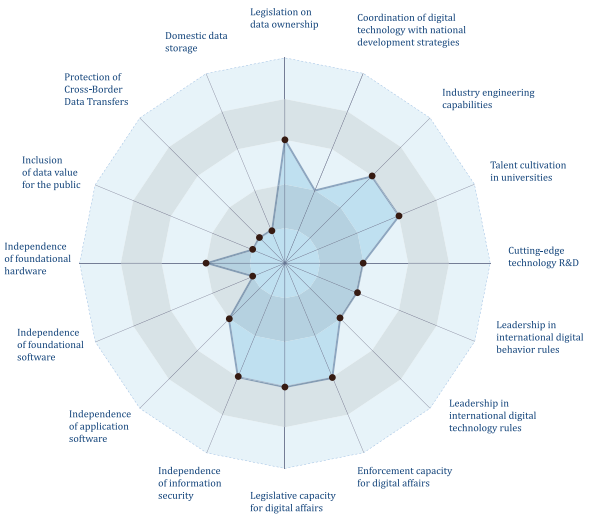
After being re-elected president, Lula announced the launch of the "New Industry Brazil" plan in January 2024, officially embarking on a new industrialization path. The plan is led by the National Industrial Development Council of Brazil, setting a series of development goals for the next decade to reverse the "deindustrialization process" that has affected Brazil for decades. Among the plan's six priority tasks is "promoting industrial digital transformation." However, this ambitious plan faces the embarrassing situation of simultaneous shortages of both investment and technology elements. Long-term privatization and liberalization of the domestic information industry has led to problems such as lack of industry autonomy, insufficient reserves of scientific research and engineering capabilities, and weak policy guidance, constraining the implementation of the transformation plan.

In summary, the Lula government has shown ambition from the perspective of national development strategy to revitalize the digital industry and promote digital transformation. However, Brazil's ICT industry has lacked policy support since the 1990s, with relatively weak digital technology capabilities and considerable room for improvement in coordination with national development strategies. However, the government must work hard to counter the lobbying of big tech companies and neoliberal theory, which hinder the implementation of sovereign technology policies. In particular, if the problems of investment and technology shortages cannot be effectively resolved, they will cause major obstacles to the implementation of industrial digital transformation. Currently, Brazil's central bank benchmark interest rate is still as high as 10.5%, with a still obvious inhibitory effect on industrial investment. It can be expected that the Brazilian government will face many challenges in solving the two major shortages of investment and technology in the digitalization field. The authors' evaluation of Brazil on the indicator of "coordination of digital technology with national development strategies" is "2 - Aware."

Coordination of digital technology with national development strategies — 2 - Aware

Conclusions and Outlook

In summary, Brazil's Digital Sovereignty Index assessment results are shown below:



Brazil's Digital Sovereignty Index Assessment Results

It can be seen that Brazil's overall digital sovereignty level is still relatively weak. None of the 16 indicators have reached the "4 - Competent" level, meaning it cannot quickly break away from dependence on foreign countries (mainly the United States) and transition to an independent and autonomous state when necessary. The promulgation of the LGPD reflects the country's significant legislative progress in data protection, and some achievements have been made in the implementation of data protection and information security. However, problems such as small industrial scale, weak R&D capabilities, lack of policy orientation, and leadership by state-owned enterprises constrain Brazil from achieving greater autonomy in digital infrastructure and international digital governance.

The policy shift since the 1990s has undermined the foundation for sustained development of the digital industry, which is the main cause of the country's currently low level of digital sovereignty. Looking ahead, extensive and in-depth cooperation with China may to some extent make up for Brazil's shortcomings in digital R&D and engineering capabilities and reduce its dependence on the United States for digital infrastructure. However, in the long run, increasing investment in STEM education and industrial engineering capabilities, cultivating a pool of talent with digital skills, and building a group of state-owned enterprises capable of implementing national development strategies may be the fundamental cure for Brazil to enhance its digital sovereignty level.

Russia Digital Sovereignty Index Assessment Report

Russia is one of the earliest countries to alert the international community to the importance of information sovereignty. Since 1998, Russia has been actively advocating for the development of rules for responsible state behavior in the information domain, with due consideration for the sovereignty and independence of each country and the equality of their rights. Since 2014, Russia has been subjected to extensive sanctions from the West, a situation that has further intensified after 2022, which has also prompted Russia to accelerate its pursuit of digital sovereignty. The escalating geopolitical pressure and Western sanctions since 2014 have powerfully driven Russia's quest for digital sovereignty. Russia already possesses relatively strong independent capabilities or international competitiveness in application software, foundational software, information security, and talent cultivation. However, Russia also has significant shortcomings: there are serious "chokepoint" problems in foundational hardware (especially chips); the theoretical understanding of data value and practices to benefit the public are still in their initial stages; enforcement capabilities against foreign tech giants remain weak; and its influence in the international digital technology and behavioral rules-setting system is extremely limited due to its exclusion. In addition, the deindustrialization process after the collapse of the Soviet Union has created long-term obstacles to Russia's current ICT industry capabilities.

Driven by an increasingly strengthened sovereignty consciousness, Russia's domestic ICT industry is experiencing new development opportunities. If Russia can deepen strategic cooperation with China and other Global South countries within the BRICS framework in the future to jointly break through technological blockades, Russia has the potential to fully master its digital sovereignty in the not-too-distant future. Below, I will use the Digital Sovereignty Index measurement system to assess Russia's level of digital sovereignty. This assessment is based entirely on publicly available information.

Russia Data Ownership Independence Status

1.1. Legislation on data ownership

Russia's most important legislation on data ownership is the Federal Law "On Personal Data" (152-FZ, also known as the Data Protection Act, abbreviated as DPA) promulgated in July 2006. This law applies broadly to any entity (including individuals and organizations) that processes the personal data of Russian citizens, regardless of their location.

The DPA defines personal data as "any information that can be used to directly or indirectly identify a specific individual." This broad definition covers a quite extensive range of data types, including basic identity information, physical and biometric characteristics, professional and financial information, online data, and more. It is worth noting that according to the law, even "indirectly identifiable information" is considered personal data. This means that seemingly anonymous data can be combined with other information to identify individuals. For example, combinations of IP addresses, browsing history, and location data can be used to identify specific individuals and therefore fall within the category of "personal data." This definition is overall similar to the GDPR's definition of personal data.

The DPA regulates the behavior of personal data processors regarding obtaining consent, collecting data, storing and using data, ensuring data security, and cross-border data transfer. This article will discuss the issues of data storage and cross-border flow in more detail later.

The DPA contains a series of enforcement mechanisms and penalties to ensure compliance with its provisions. These actions aim to deter violations, punish non-compliant behavior, and incentivize organizations to handle personal data responsibly. However, the penalties stipulated are actually quite light. For example, according to amendments passed in December 2023 (589-FZ), the maximum fine for "processing personal data without the consent of the data subject" is only 1.5 million rubles (approximately $15,000). For internet companies that collect large amounts of personal data, this fine amount is undoubtedly too low and can almost be said to encourage illegal data collection. The State Duma is reportedly considering raising the maximum fine for data processors who abuse or cause personal data leaks to 3% of previous year's revenue and not exceeding 500 million rubles (approximately $5 million). Even if this adjustment becomes reality, this penalty level is not in the same order of magnitude as the EU (up to 4% of previous year's revenue) and China (up to 5% of previous year's revenue), and cannot form a deterrent against internet giants at all.

From several actual penalty cases, the penalties imposed on internet giants such as Zoom (1 million rubles, approximately $10,000), Apple (2 million rubles, approximately $20,000), and Google (15 million rubles, approximately $150,000) for violating DPA-related provisions are indeed too low.

The main agencies responsible for enforcing data protection are the Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Minkomsvyaz) and the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor). However, from the penalty cases against several American internet giants, it appears that enforcement authority is exercised by district courts in Moscow. The decentralization of enforcement authority may also be one of the factors contributing to light penalties.

In summary, Russia's Data Protection Act (DPA) has many similarities with the EU's GDPR, forming a legal foundation for protecting individual and national data ownership. However, there are relatively few penalty cases based on the DPA, and the penalties are relatively light. This is partly due to the provisions of the DPA itself, and partly may be related to the decentralized enforcement authority and the lack of a strong national-level enforcement agency. Based on the above information, on the indicator of "Legislation on data ownership," I give a rating of "Level 4: Competent."

Legislation on data ownership — Level 4: Competent

1.2. Domestic data storage

In July 2014, Federal Law No. 242-FZ "On Amending Certain Legislative Acts Concerning the Updating of Procedures for Personal Data Processing in Information-Telecommunication Networks" amended the Per-

sonal Data Act (DPA) and the Information Act formulated in 2006. The amendments require all data operators to ensure that any recording, systematization, accumulation, storage, alteration, or retrieval of personal data of Russian citizens be conducted in data centers located within the territory of the Russian Federation. This means that any personal data of Russian citizens collected by data operators must be stored on servers, IT systems, databases, or data centers located within the territory of the Russian Federation; and introduces new mechanisms for the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) to block websites and network resources that illegally process Russian citizens' personal data.

This rule does not prohibit storing and processing Russian citizens' personal data outside of Russia, as long as the primary (usually interpreted as initial) storage and other processing activities as stipulated by the DPA are conducted within Russia. Relevant provisions regarding cross-border data transfer are separately stipulated in other parts of the DPA. The penalty for violating this provision is ultimately blocking websites involved in illegal processing of Russian personal data and imposing a fine of up to 6 million rubles (approximately $60,000), with repeat offenders subject to a maximum fine of 18 million rubles (approximately $180,000).

Russian enterprises generally have no objection to complying with data localization regulations. For example, one of the selling points of Russian tech company Yandex's cloud services is that it can help enterprises comply with localization laws. However, many foreign companies such as Twitter, Google, and Facebook have long ignored localization requirements and occasionally pay relatively small fines (sometimes only tens of thousands of dollars, which is a drop in the bucket compared to their profits). Since 2022, the United States has further strengthened sanctions against Russia, and major American internet companies are even less likely to establish local data centers in Russia. Currently, the most popular search engine in Russia is the domestic Yandex (with about 72.4% market share), followed by Google (about 26.2%). WhatsApp (which belongs to the same parent company Meta as Facebook) is the most popular social media application, with user coverage reaching 74.5%. To date, the Russian government has not yet found a way to force these foreign companies to comply with data localization-related legal provisions.

In summary, Russia has formulated clear data localization provisions since 2014, and domestic enterprises have executed these provisions well. However, American internet giants still have quite high market shares in the Russian market and have shown no willingness to localize data, and the Russian government has not taken strict measures against them. It is currently unclear whether Russia is prepared to risk the complete withdrawal of American internet giants to enforce data localization provisions. On the indicator of "Domestic data storage," I give a rating of "Level 3: Developing."

Domestic data storage — Level 3: Developing

1.3. Protection of cross-border data transfers

As mentioned earlier, Russia's data localization requirement is only "mirroring" (i.e., maintaining a copy of personal data within Russia), rather than stricter "hard localization" (i.e., in principle not allowing personal data to leave the country). According to relevant provisions of the DPA, before transferring personal data collected within Russia abroad, data controllers must proactively register and notify Roskomnadzor of cross-border data transfers.

According to DPA provisions, the party receiving data abroad must provide adequate protection for personal data. This can be achieved through various mechanisms: adequacy decisions, standard contractual clauses, binding corporate rules, etc. Data exporters must conduct technical impact assessments for all destination countries in all circumstances. If the destination of data transfer is a "country that adequately protects personal data," the evaluation and review process for data transfer is greatly simplified, for example, it does not need to include a review of that country's laws. The so-called "countries that adequately protect personal data" mainly refer to the 55 signatory countries of the Council of Europe's "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (ETS No. 108) signed in 1981, and the 29 whitelist countries separately listed in Roskomnadzor's Order No. 274 in 2013 — neither the United States nor China are on these two lists.

The relevant legal provisions on cross-border data transfer also suffer from insufficient enforcement. For Facebook and Twitter's violations in transferring data abroad, the Tagansky District Court in Moscow

imposed fines of 3,000 rubles (approximately $30). Facebook did not even send a representative to court. Internet companies penalized for the same reason also include WhatsApp (18 million rubles), Tinder (2 million rubles), Snap and Hotels.com (1 million rubles each), etc. Compared to the 8 billion yuan (approximately $1.1 billion) fine issued by China to the ride-hailing platform DiDi for illegal cross-border data transfer, the fines issued by Russian courts clearly lack deterrent power against internet giants.

In summary, Russia has formulated laws for cross-border data flows, but enforcement is relatively light, lacking deterrent power against foreign companies, especially American internet giants. The low level of independence in Russia's digital infrastructure and the lack of alternatives to these American internet platforms, making it impossible to ban these American platforms, may also be factors contributing to weak enforcement. On the indicator of "Protection of cross-border data transfers," I give a rating of "Level 3: Developing."

Protection of cross-border data transfers — Level 3: Developing

1.4. Inclusion of data value for the public

Regarding how to understand the value of data, a relatively mature theory in the economic sense has not yet been formed in Russia. In 2022, the Central Bank of Russia suggested discussing the possible circulation of digital assets in exchange trading, methods to coordinate taxation of digital assets with traditional financial instruments, conditions for individual institutional investors to access digital assets, and the establishment of accounting procedures for such investments. These discussions primarily revolved around digital assets such as cryptocurrencies based on blockchain technology.

As of early 2024, Russia has approximately 130 million internet users, with an internet penetration rate of 90.4%; among them, 106 million social media users, equivalent to 73.5% of the total population. The data continuously produced by this scale of users is itself an asset with economic value — this means that this data itself should be able to be valued in an accounting sense, included in the balance sheet of its owners, thereby increasing the economic value of data owners.

However, Russia's theoretical understanding of data value has not yet reached this level. In the "Digital Economy Program of the Russian Federation" released in 2017, data is referred to as "a key factor of production in the digital economy," but the program and subsequent policy documents do not elaborate on the substantive questions of why data is treated as a factor of production and how to treat this factor of production. Several American internet giant companies continue to extract data from Russia, which may be related to this insufficient understanding of data value and subsequent insufficient attention to data ownership.

Based on this theoretical understanding, to my knowledge, regarding the issue of internet giants appropriating the data value created by users without compensation, Russia has not yet formed systematic criticism, nor are there discussions on how to return data value to the public. On the indicator of "Inclusion of data value for the public," I give a rating of "Level 1: Initial."

Inclusion of data value for the public — Level 1: Initial

Russia Digital Infrastructure Independence Status

Russia's ICT (information and communication technology) market size in 2023 was $38.06 billion, or $263.9 per capita. This market volume and per capita market volume rank second to last among the BRICS five countries: total volume is only higher than South Africa, and per capita volume is only higher than India. Although it partly inherited the Soviet Union's technology and industrial capabilities, the relatively small market size has prevented Russia from forming a complete and independent ICT industry. On the other hand, since the release of the "Digital Economy Program" in 2017, Russia's ICT market has grown rapidly, with the compound annual growth rate (CAGR) after 2023 expected to reach 9.14%, and the total market volume projected to reach $58.94 billion by 2028. At the same time, the tense geopolitical situation has actually provided development opportunities for Russia's domestic ICT industry, and the overall trend of digital infrastructure independence is positive.

2.1. Independence of foundational hardware

The Digital Sovereignty Index primarily examines the level of independence in three types of foundational hardware: chips, servers, and storage devices.

Russia had two companies that independently developed computer microchips: Baikal Electronics and the Moscow Center of SPARC Technologies (MCST). Baikal's parent company is T-Platforms, founded in 2002, which was part of a Russian government program focusing on supercomputer research and development. The Lomonosov supercomputer developed by T-Platforms in 2011 with 33,072 processors ranked 18th in the world and third in Europe at the time, and was also Russia's fastest supercomputer. In 2021, CPUs designed by Baikal had reached the performance of Intel's low-end CPUs from 2017 and could be used for general office and home computers. At that time, Baikal planned to have TSMC produce 15,000 CPUs per month, paired with the domestically produced Astra Linux operating system, to achieve replacement of the Wintel architecture within government and state-owned enterprises. After 2022, TSMC stopped cooperating with Baikal, and the company had to seek 28-nanometer chip manufacturing capabilities domestically, a process that proved to be very difficult. In 2023, Baikal, along with its parent company T-Platforms, went bankrupt.

Another chip manufacturer, MCST, was established in 1992 as a subsidiary of the Lebedev Institute of Precision Mechanics and Computer Technology — the institute was formerly affiliated with the Soviet Academy of Sciences and was transformed into a joint-stock company in 2009. MCST uses its own developed Elbrus instruction set architecture, which employs the Very Long Instruction Word (VLIW) approach. This instruction set architecture is completely different from the general-purpose CPUs currently popular in the market and is not suitable for the mass market. The Elbrus chips developed based on this instruction set are designed according to the Russian government's requirements for security and reliability and are only supplied to customers designated for national sensitive work, such as the Ministry of Internal Affairs and some oil and gas companies. The state-owned enterprise Rostec has developed a series of specialized computers based on Elbrus chips, including a single-board computer that is only 95×95 millimeters in size. MCST also relied on TSMC for chip production, which ceased supplying MCST in June 2023.

The current reality is that, despite being jointly sanctioned by Western countries, Russia's chip supply remains highly dependent on the United States and Europe. According to Bloomberg reports, in the first nine months of 2023, Russia imported more than $1 billion worth of chips from the United States and Europe, with suppliers including major companies such as Intel, AMD, and ADI. To break free from this dependence, the Ministry of Industry and Trade of Russia and the Moscow Institute of Electronic Technology (MIET) have formulated a large-scale plan for import substitution of electronic production equipment, aiming to achieve a 70% import substitution rate for microelectronic production equipment and materials by 2030. To this end, the state will launch 110 R&D projects, investing more than 240 billion rubles (approximately $2.4 billion).

One major Russian server manufacturer is Jahont, which provides servers with built-in Elbrus processors and Astra Linux operating systems for document management systems in public institutions (Jahont-YVM E12) and in the healthcare sector (Jahont-EMK). Some enterprises in the energy sector are also considering using completely self-sufficient domestic servers to run their ERP systems. Russian domestic cloud service provider Yandex invested in a domestic server manufacturer called OpenYard in 2021, which began production at the end of 2023, expecting to produce 60,000 x86 architecture servers per year. After server manufacturers Dell, Cisco, HP, and other companies closed their operations in Russia, large companies in the internet, oil, banking, and other industries have had to procure second-hand servers to meet their IT needs.

According to a research report by the German Council on Foreign Relations, Russia currently has no independent capacity to produce memory chips and storage drives and is completely dependent on foreign manufacturers.

In summary, due to Western sanctions, Russia has an urgent need for foundational hardware independence, but existing production and supply chain capabilities have obvious shortcomings and cannot currently meet the demand. Although it has inherited part of the Soviet Union's technology and industrial capabilities, and the state has invested resources to build an independent import substitution industry, whether the investment scale matches the importance and urgency of foundational hardware independence still requires

observation — as a comparison, China's National Integrated Circuit Industry Investment Fund Phase III established in 2024 has an investment scale of 344 billion yuan (approximately $47.56 billion). I evaluate Russia on the indicator of "Independence of foundational hardware" as "Level 3: Developing."

Independence of foundational hardware — Level 3: Developing

2.2. Independence of foundational software

The Digital Sovereignty Index primarily examines the level of independence in four types of foundational software: operating systems, databases, middleware, and cloud platforms.

The Astra Linux operating system developed by Russian software company RusBITech based on Debian has been deployed in many government departments and the military since 2018 and has been proven to be capable of replacing Microsoft's Windows operating system. The Astra operating system can run on ARM, Intel, and Russia's domestically produced Elbrus architecture, and also provides a free version for ordinary users. There is a statistic showing that the Linux operating system's market share in Russia is only 1.66%, far lower than Windows (53.89%) and OS X (4.45%). I believe that the Astra operating system used by government and military may not be included in this statistic, thus underestimating the usage of Linux operating systems.

The absolute dominant players in Russia's mobile operating system market are two American companies: Google (Android, with 72% market share) and Apple (iOS, with 27.5% market share). Rostelecom has independently developed the Aurora mobile operating system based on the Linux kernel. Many mobile devices of employees of Russian Railways, Russian Post, and Rostelecom have Aurora operating system installed. It was also installed on hundreds of thousands of tablets involved in the nationwide population census in autumn 2021. It is expected that work phones and tablets used by employees of government agencies, state-owned enterprises, and critical infrastructure will be mandatorily installed with the Aurora system. Aurora is also developing versions for smart TVs, smart cars, payment terminals (POS), and other scenarios, aiming to fully enter the consumer market and gradually replace Android and iOS. However, Rostelecom also faces difficulties in obtaining chips due to sanctions when producing smart devices based on the Aurora operating system. In November 2022, Rostelecom proposed a project to build a mobile ecosystem based on the Aurora operating system, planning to invest 480 billion rubles (approximately $4.8 billion) by 2030 to release about 70 million smartphones based on the Aurora system. Some analysts believe this plan will involve cooperation with Chinese mobile phone manufacturers.

In the database field, Russia has strong industrial capabilities based on open-source databases. According to statistics, 82% of software companies use the open-source PostgreSQL, far exceeding the major commercial database products MS SQL (47%) and Oracle (24%). Russian enterprises engaged in data management business generally view Western sanctions and the withdrawal of Western large software companies as opportunities. A manager at software company IBS believes that almost all foreign products in this field have alternatives. Companies such as ArenaData and Red Soft have developed their own data products based on open-source technologies like PostgreSQL and MongoDB. Some large Russian banks, including VTB, Rosbank, and OTP Bank, have migrated to data management solutions provided by local suppliers. Some private enterprises have also begun to shift to using domestically developed data management solutions, claiming this can optimize data processing workflows. The market demand in Russia's data management and processing field is expected to reach 170 billion rubles (approximately $1.7 billion) by 2027, triple the 2022 figure.

I have not found relevant information about Russia's independent middleware capabilities. Given that middleware (compared to operating systems and databases) has relatively lower R&D technical difficulty, I believe it can be reasonably inferred that if subject to Western sanctions, Russian enterprises have the capability to independently develop most middleware. For example, medical IT company Mitra has developed middleware products for medical equipment.

The state-driven digitalization program has brought growth momentum to infrastructure cloud services. In 2023, Russia's infrastructure cloud services (IaaS) market size was 121 billion rubles (approximately $1.21 billion), a year-on-year increase of 33.9%. Meanwhile, Western sanctions have forced American cloud service

providers such as Microsoft Azure, Google Cloud, and AWS to exit the Russian market, replaced by domestic enterprises such as Rostelecom (23.7% IaaS market share), Cloud.ru (21.8%), Yandex.Cloud (9.8%), Selectel (7.2%), and MTS (6.2%). Russia's cloud computing adoption started relatively late, and the market is still very underdeveloped. Its per capita cloud service market size (approximately $8.41) is only about 10% of China's (approximately $82.59). It can be expected that this market still has great growth potential, and American companies have completely lost this market.

In summary, Russia has certain independent capabilities in foundational software such as operating systems, databases, and middleware, and has achieved a relatively high level of independence in cloud computing. The withdrawal of Western companies from the Russian market due to geopolitical factors has instead provided rare development opportunities for domestic companies. With the joint efforts of government and enterprises, Russia's domestically produced foundational software already has the potential to fully replace imported software and has the prospect of gaining greater development space in the future. I evaluate Russia on the indicator of "Independence of foundational software" as "Level 4: Competent."

Independence of foundational software — Level 4: Competent

2.3. Independence of application software

The Digital Sovereignty Index primarily examines a country's application software independence from three perspectives: office software, general software, and industry software.

In his annual address to the Federal Assembly in 2014, President Putin reiterated that "we must reduce our serious dependence on foreign technology" and that "the import substitution program must encourage the creation of a large number of industrial enterprises that are competitive not only domestically but also in international markets." Compared to the hardware field, Russia's capabilities in software development are much stronger, with numerous IT companies developing software products suitable to the country's conditions, including some world-renowned software companies. As of the end of 2023, the registry of domestic software established by the Russian government had more than 7,000 companies and 18,800 domestic software products.

MyOffice is the Russian alternative to Microsoft Office software, providing the main functions of Microsoft Office such as processing text documents, spreadsheets, presentation slides, sending and receiving emails, and calendar management. It also provides online cloud services similar to Microsoft Office 365, and its price is less than half of Microsoft Office. In 2021, 77.5% of the Russian office software market was occupied by foreign products, with domestic software accounting for only 7% market share. Since 2022, this situation has changed rapidly, with the market share of domestic software rising sharply. It is predicted that by 2027, domestic office software will occupy 82% of Russia's market share. In addition, since 2019, MyOffice has gradually promoted its products to African markets. The Minister of Basic Education of Cameroon pointed out that MyOffice does not need to send data to company servers abroad, thus better protecting data privacy.

Application software for personal use such as search engines (Yandex, Rambler), email services (Mail.ru), and social networks (VK, Odnoklassniki) all have mature companies operating in Russia. Yandex has already captured 70% of the search market.

Since the second quarter of 2022, internationally renowned ERP vendors such as SAP, Oracle, and Microsoft have exited the Russian market, and Russian enterprises have fully shifted to using domestic ERP software. Large enterprises that have already implemented ERP systems also face urgent pressure for domestic substitution to break away from dependence on Western software vendors and avoid the risk of operational data being controlled by Western governments, thereby increasing demand for domestic ERP software. The most leading domestic ERP is 1C ERP. Among the more than 400 ERP implementation projects between 2021 and 2023, 68.6% adopted the 1C solution, followed by SAP (5.6%) and Microsoft (4.5%).

Various types of industry software also have corresponding enterprises providing domestic alternative solutions. For example, MES systems are provided by companies such as RTSoft, Galaktika, and Konsom Grupp, and SCADA systems have domestic software such as SCADA-KRUG, MasterSCADA, IntraSCADA, and RapidSCADA.

A lesser-known fact is that thanks to the Soviet Union's technology and talent accumulation, Russia has very strong technical capabilities in the most technologically demanding R&D and design industrial software (such as CAD) in industrial software. French company Dassault Systèmes cooperated with Russian research institutions in a series of projects in the 1990s, which played an important role in promoting the early development of its CAD products. CAD software such as TurboCAD, BricsCAD, and IntelliCAD were all developed in Russia. ASCON, founded 35 years ago and headquartered in St. Petersburg (then still called Leningrad), developed the KOMPAS series of CAD software that was used for fuselage modeling of the MiG-29 fighter and is currently widely used by more than 7,000 industrial and engineering organizations worldwide in mechanical, automotive, electronics, shipbuilding, atomic energy, aerospace, defense, plant design, civil engineering, and construction fields.

In summary, Russia has considerable strength in the application software field. After Western companies withdrew from the Russian market due to geopolitical factors, domestic companies have gained rare development opportunities and have basically achieved complete independence in this field. I evaluate Russia on the indicator of "Independence of application software" as "Level 5: Independent."

Independence of application software — Level 5: Independent

2.4. Independence of information security

The information security pressure Russia faces may be the greatest among all countries. In 2024 alone, Russia's financial system, power grid, media, and government departments have all suffered large-scale hacker attacks. The fact that dozens of Iranian websites were blocked by the US government and ICANN, which is responsible for managing internet domain names and IP address allocation, in 2021 also made Russia worry that its websites could "disappear" in the same way at any time.

In the field of cybersecurity, Russia has many competitive companies, such as Kaspersky and Positive Technologies. Founded in 1997, Kaspersky is one of the world's top antivirus and cybersecurity companies, and its founder Eugene Kaspersky once worked for the Federal Security Service. The company currently has more than 270,000 corporate clients and over 400 million users worldwide, with global revenue of $721 million in 2023. Kaspersky has close cooperation with the Russian government and has disclosed cyberattacks against the Russian government on multiple occasions. In July 2024, Kaspersky ceased operations in the United States because the Biden administration banned the sale and distribution of the company's software. Another major Russian information security company, Positive Technologies, is the organizer of the internationally renowned hacker conference Positive Hack Days. Despite also being sanctioned by the United States, the company achieved double-digit revenue growth in 2023 and is expected to achieve more international revenue growth in 2024.

In a dialogue held at the 2023 Positive Hack Days conference, experts pointed out that Russia still lacks viable alternatives in underlying software development technologies (such as kernels, compilers, interpreters, etc.) and lacks control over the open-source supply chain, which poses potential risks to Russia's information security. In May 2022, Maksut Shadayev, Minister of Digital Development, Communications and Mass Media of the Russian Federation, announced plans to transform the domestic software registry into a software solutions marketplace to simplify user access to domestic software. However, I believe this measure is not yet sufficient to address possible open-source supply chain attacks.

In response to potential attacks on internet root servers, Russia has been building a domain name system and infrastructure managed by Roskomnadzor since 2018, to some extent replacing the global domain name system currently managed by ICANN. However, given that ICANN still holds management rights over global internet root nodes, in extreme situations, Russia's independent domain name system still cannot prevent the risk of its domestic websites being isolated from the global internet.

In summary, under the pressure of real cybersecurity threats, thanks to deep technical strength accumulated over many years, Russia has developed a basically independent defensive information security system. However, for some attack methods utilizing internet underlying mechanisms controlled by the United States, Russia currently still lacks countermeasures. I evaluate Russia on the indicator of "Independence of information security" as "Level 4: Competent."

Independence of information security — Level 4: Competent

Russia Digital Governance Independence Status

3.1. Legislative capacity for digital affairs

Due to geopolitical pressure, most of Russia's legislation on digital affairs in recent years has been focused on information security and national security. In the large-scale anti-government demonstrations and protests that erupted in December 2011, American internet platforms played an important mobilization and organizational role. Subsequently, the Russian government conducted a series of legislation on digital space governance, including N398-FZ (the "Lugovoi Law") promulgated in 2013 on restricting extremist content websites, N242-FZ (the "Data Localization Law") promulgated in 2014 stipulating that domestic data must be stored domestically, N374-FZ (the "Yarovaya Law") promulgated in 2016 detailing data localization storage rules, N276-FZ promulgated in 2017 on prohibiting the use of anonymizers and VPNs to access blocked websites, N90-FZ (the "Sovereign Internet Law") promulgated in 2019 on strengthening internet sovereignty, N511-FZ and N482-FZ promulgated in 2020 on website content review, and N236-FZ promulgated in 2021 requiring internet companies with more than 500,000 Russian users to open representative offices in Russia. Reviewing this legislation, it can be seen that the focus is on strengthening sovereign governance of cyberspace and preventing potential attacks by external forces through cyberspace.

On the other hand, Russia's legislation serving digital economy development is relatively lacking. Since the launch of the National Digital Economy Program in 2018, the specific implementation of the program has not been further refined in the form of legislation or mandatory national standards. Some common problems and tasks that may be encountered in the development of the digital economy, such as recommendation algorithm regulation, protection of labor rights in the platform economy environment, prevention and governance of monopolies by internet platform companies, and ethical issues in artificial intelligence development, have not been implemented as corresponding legislation. One impact of the lack of detailed national planning is that its implementation progress and effects are prone to deviate from the original plan. For example, information infrastructure construction is the sub-project with the largest planned investment and the most importance in the National Digital Economy Program, and the development of 5G communication networks is an important component of this sub-project, but the development of 5G has encountered obstacles, and the timeline for large-scale commercial implementation has been repeatedly delayed.

In July 2024, the State Duma passed two bills aimed at encouraging and regulating encrypted digital assets, including regulating cryptocurrency mining, recognizing the tradability of foreign digital copyrights and stablecoins (Bill No. 237585-8), and allowing import-export enterprises to use cryptocurrency in cross-border settlements under foreign trade agreements (Bill No. 341257-8). Analysts generally believe that the intention of these bills is mainly to seek cross-border settlement mechanisms outside the dollar.

In summary, Russia's legislation on digital affairs focuses on areas related to national security and responding to Western sanctions, with insufficient attention to legislation related to digital economy development, which to a certain extent has also affected the implementation of the National Digital Economy Program. The real geopolitical pressure Russia faces is also an important factor leading to this focus imbalance. I evaluate Russia on the indicator of "Legislative capacity for digital affairs" as "Level 4: Competent."

Legislative capacity for digital affairs — Level 4: Competent

3.2. Enforcement capacity for digital affairs

According to the N236-FZ law promulgated in 2021, foreign internet companies with more than 500,000 Russian users must open representative offices in Russia. According to Roskomnadzor's registration, there are 13 foreign companies that meet this condition, including Google, Facebook, Apple, Twitter, TikTok, and Telegram. The law officially came into effect on January 1, 2022, and stipulates various enforcement measures by authorities in case of violations, including limiting transfers and payments, slowing local traffic, and completely blocking access to online resources. From actual enforcement actions, the previous fines imposed on these foreign companies were quite small, and the ones actually banned from access were a batch of European media websites and the social network Discord, which had relatively few users. The enforcement capacity against American tech giants still needs

to be observed.

In October 2024, a Russian court issued a sky-high fine of 35-digit dollars against Google. This fine amount is so huge that it instead makes the Russian government's enforcement of digital affairs seem unserious.

I have not yet found relevant information about the Russian government's enforcement of digital affairs against its domestic enterprises.

In summary, Russia's enforcement capacity for digital affairs is still in the process of continuous improvement. I evaluate Russia on the indicator of "Enforcement capacity for digital affairs" as "Level 3: Developing."

Enforcement capacity for digital affairs — Level 3: Developing

3.3. Leadership in international digital technology rules

The technological development direction and roadmap of the ICT industry are largely influenced by international standards development organizations (SDOs). The Atlantic Council's report views the number of voting seats a country holds in several important SDOs as an important criterion for a country's dominance in technical rule-making and technological leadership position.

Among the 11 internationally important SDOs in the ICT industry that I examined, Russia has almost no voting seats — only telecom operator MegaFon and the International Organization of Space Communications (Intersputnik) headquartered in Moscow still retain membership in the International Telecommunication Union (ITU). Additionally, although the International Organization for Standardization (ISO) has not expelled Russia from key technical committees, it has indefinitely postponed all technical activities in which Russia held a dominant position within the ISO framework. I believe this phenomenon may not only be due to the intensified geopolitical conflict since 2022 but can even be traced back to the Cold War history. Regardless of its causes, the fact that a major country like Russia is almost completely excluded from the decision-making mechanism of international digital technology rule-making reflects the systemic risks existing in the current Western (especially American) dominated international digital technology rules system.

In short, the objective fact is that Russia currently has very limited influence in international SDOs, which does not match its national strength and technological level. I evaluate Russia on the indicator of "Leadership in international digital technology rules" as "Level 2: Aware."

Leadership in international digital technology rules — Level 2: Aware

3.4. Leadership in international digital behavior rules

Faced with isolation, blockade, sanctions, and weaponization of the internet by Western countries, Russia is working hard to seek participation in international digital behavior rule-making led by non-Western countries. The 2024 BRICS Leaders' Kazan Declaration states that BRICS countries are jointly committed to developing and implementing globally interoperable common rules and standards for supply chain security, preventing and combating crimes in information and communication technology, promoting respect for national sovereignty and sovereign equality in the information and communication technology environment, and opposing unilateral actions that undermine international cooperation in this field and the sustainability of global supply chains. BRICS countries will further strengthen practical cooperation on cybersecurity and express serious concern about the exponential proliferation and spread of false information, misinformation, and hate speech on mainstream international internet platforms.

Russian academia has also organized some international conferences related to digital space governance, such as the 27th International Joint Scientific Conference "Internet and Modern Society" (IMS-2024) held in St. Petersburg in June 2024 and the Third International Scientific-Practical Conference "Digital International Relations 2024" held in Moscow in October 2024. Based on my observation, the main significance of these international conferences at present is to maintain dialogue between researchers in Russia and researchers in other countries in related fields, and the achievements are not yet clear.

In summary, Russia is currently working hard to break free from Western blockades and seeking entry points to participate in international digital behavior rule-making in the Global South. I evaluate Russia on the indicator of "Leadership in international digital behavior rules" as "Level 2: Aware."

Leadership in international digital behavior rules — Level 2: Aware

Russia Digital Capability Independence Status

4.1. Cutting-edge technology research and development

According to the World Intellectual Property Organization (WIPO) patent technology classification, Category I "Electrical Engineering" (including 5 subcategories: 1. Electrical machinery, apparatus, electrical energy; 2. Audio and video technology; 3. Telecommunications; 4. Information technology; 5. Semiconductors) can basically be considered equivalent to digital industry-related technologies. The number of patents a country obtains in this major category can, to a certain extent, serve as an indirect indicator of that country's technological R&D and innovation capabilities in the digitalization field.

In 2021, among the more than 560,000 international patents granted in Category I, Russia accounted for 1,973, representing 0.35%, ranking 14th in the world, behind Finland, Switzerland, and other countries. This data is not much different from the 2013 data. In 2022, the number of international patents Russia obtained in this major category sharply decreased to 706 (0.12%); in 2023, this number dropped even more dramatically to 185 (0.03%). It can be seen that Western blockades have greatly affected Russia's international patent applications.

From the 2021 international patent data, Russia has a large gap with China (224,000, 39.84%), the United States (118,000, 21.11%), Japan (88,000, 15.74%), and South Korea (66,000, 11.76%), and also has a significant gap with traditional European powers such as Germany (15,000, 2.66%), France (8,516, 1.52%), and the United Kingdom (5,607, 1.00%), although it still leads major Global South countries such as India (1,667, 0.30%), Brazil (202, 0.04%), and South Africa (43, 0.01%). I believe this data basically objectively reflects Russia's current input and output in cutting-edge digital technology.

It is worth mentioning that although the number of patents is relatively small, Russia has its unique advantages in some highly technical fields such as high-end industrial software (introduced earlier), information security, and supercomputers. However, Western technological blockades have also hindered Russia's pace of scientific and technological innovation. Taking all factors into comprehensive consideration, I evaluate Russia on the indicator of "Cutting-edge technology research and development" as "Level 3: Developing."

Cutting-edge technology research and development — Level 3: Developing

4.2. Talent cultivation in universities

According to OECD data, in 2020, the total number of university graduates in science, technology, engineering, and mathematics (STEM) disciplines in Russia was 520,000, second only to China (3.57 million), India (2.55 million), and the United States (820,000), more than double Brazil's (238,000); STEM graduates accounted for 37% of all university graduates, second only to China (41%). The educational tradition left from the Soviet era continues to supply a steady stream of potential digital talents to today's Russia, but whether these university graduates can enter the digitalization industry mainly depends on the employment capacity created by the ICT industry. I evaluate Russia on the indicator of "Talent cultivation in universities" as "Level 4: Competent."

Talent cultivation in universities — Level 4: Competent

4.3. Industry engineering capabilities

In 2012, the total number of ICT practitioners in Russia did not exceed 300,000; this number grew to 1.93 million by 2022, roughly equivalent to Brazil. However, compared to Brazil, Russia has a group of enterprises

with relatively high technical content and independent R&D capabilities, as well as software companies and internet companies serving the domestic market, some of which (such as Kaspersky, Yandex, ASCON, etc.) possess world-class competitiveness. I believe that under the backdrop of the state vigorously promoting digitalization and Western companies comprehensively withdrawing from the Russian market, Russia's talent advantages will continue to be transformed into ICT industry engineering technical capabilities in the future. Therefore, I evaluate Russia on the indicator of "Industry engineering capabilities" as "Level 4: Competent."

Industry engineering capabilities — Level 4: Competent

4.4 Coordination of digital technology with national development strategies

In 1950, the Electronic Systems Laboratory of the Energy Institute of the Soviet Academy of Sciences took the lead in developing semiconductor electronic computers — at that time, computers in Britain and the United States were still in the vacuum tube era, not only huge in size but also with very high failure rates. In 1952, the M-1 computer developed by the Soviets was put into use. This was the world's first small computer based on semiconductor diode logic circuits. Throughout the Cold War period, the Soviet Union relied on independent research and development to keep up with the United States in information technology and produced world-class computer scientists like Victor Glushkov. In 1958, the Soviet Union developed the world's first fully automatic mobile telephone communication system "Altai," much earlier than Motorola's mobile phone developed in 1973 — by the mid-1970s, the "Altai" system had been promoted and operated in 114 Soviet cities. Even in the 1980s, when the world entered the personal computer era, the Soviet Union had independently developed products such as the "Agat" personal computer and the Elektronika MS 1504 laptop computer.

The collapse of the Soviet Union interrupted Russia's path to independently developing information technology. Russia once hoped to integrate into the Western-led globalization market, and the past technology and talent accumulation were also transformed to a certain extent into industrial capabilities under the market economy system, cultivating well-known software companies such as Kaspersky, 1C, ABBYY (later relocated to the United States), and Paragon Software (later relocated to Germany), as well as software outsourcing companies serving the West such as Auriga (later relocated to Germany). In 2013, four Russian cities (Moscow, St. Petersburg, Nizhny Novgorod, and Novosibirsk) made Bloomberg's list of "World's Top 100 Software Outsourcing Cities," and 9 companies made Global Services' list of "Global Top 100 Outsourcing Companies."

Since 2014, the sharply increased geopolitical pressure has shattered Russia's illusion of "integrating into the West," and Russia has begun to attach importance to the independence of digital technology and digital space governance. In 2017, President Putin approved the new "Information Society Development Strategy," which aims to guide the development of information and communication technology policy until 2030. The National Digital Economy Program launched in 2018 provided clearer goals for this strategy. In addition, Russia established the "National Technology Initiative" in 2016, aiming at new global markets in the next 15-20 years, conducting forward-looking incubation of high-tech enterprises. Currently, 74 projects have received funding from the foundation established by this initiative.

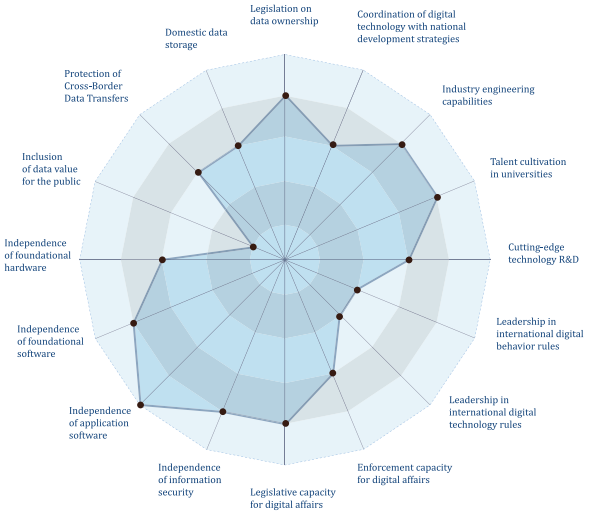
The further intensified geopolitical pressure and comprehensive Western blockade and sanctions in 2022 are both challenges and opportunities for Russia. The digital industry that has not yet achieved complete independence faces difficulties of being "choked," while the comprehensive withdrawal of Western companies is good news for the domestic industry.

Overall, Russia's current digital technology development vision is consistent with national strategic direction, and there is relatively good interaction between technological development and policy guidance. However, limited by objective conditions, the development strength and management refinement of digital technology still cannot meet the country's urgent needs. I evaluate Russia on the indicator of "Coordination of digital technology with national development strategies" as "Level 3: Developing."

Coordination of digital technology with national development strategies — Level 3: Developing

Conclusion and Outlook

In summary, the results of Russia's Digital Sovereignty Index assessment are shown in the figure below:



Russia's Digital Sovereignty Index Assessment Results

Regarding Russia's development in the digitalization field, Western researchers mostly focus on two points: controlling the internet and valuing digital assets (especially cryptocurrencies). Undoubtedly, these two points are direct responses to Russia's current enormous geopolitical pressure, but if one believes that Russia's digitalization efforts are all used to combat internet information warfare and break through dollar blockades, this view is narrow and biased. In fact, the greater significance of geopolitical pressure is that it has shattered Russia's post-Cold War illusion of "integrating into the West" and alerted it to the importance of national sovereignty and digital sovereignty. Under the guidance of increasingly strengthened sovereignty consciousness, Russia's domestic ICT industry is entering a new growth cycle. If deeper strategic cooperation can be formed with China within the BRICS framework to jointly break through Western "chokepoint" blockades on some cutting-edge technologies, and export existing technologies, products, and solutions to the vast Global South countries, Russia has a good prospect of fully mastering independent digital sovereignty in the not-too-distant future.

India Digital Sovereignty Index Assessment

Assessment Date: October 15, 2025, **DSI Overall Score**: 2.94/5.0 **Country Code**: IN

Overview

India achieves a score of 2.94 out of 5 in the Digital Sovereignty Index assessment, presenting a distinctive characteristic: possessing world-class digital capabilities yet lacking corresponding digital independence. The nation cultivates 31-34% of global STEM graduates, operates the world's second-largest technology workforce (5.43 million IT workers), has enacted comprehensive digital governance legislation comparable to GDPR, achieved world-leading innovation in payments (UPI processes 50% of global digital transactions), and demonstrated enforcement capacity against resistant foreign tech giants (Twitter compliance rate increased from 11% to 100%). Digital Governance Independence is the strongest dimension (3.5 points), with legislative capacity reaching Level 4 (Competent), and enforcement capacity and international rules leadership reaching Level 3 (Developing).

However, these excellent capabilities have not translated into comprehensive sovereignty. India imports 95% of semiconductors, faces 65% market dominance by foreign cloud providers, has less than 5% domestic share in foundational software (operating systems, databases, middleware), experiences 72.3% talent drain to US H-1B visas, and the flagship Digital Personal Data Protection Act remains non-operational 18 months after enactment. The core challenge is the capability-sovereignty deployment gap: the capabilities of 5.43 million IT workers, 2.6 million annual STEM graduates, and 64,480 patents (6th globally) primarily flow toward serving foreign markets (59.3% service exports, 72.3% talent outflow) rather than building domestic digital independence.

Dimension 1: Data Ownership Independence (2.25/5.0)

India's data governance independence presents a combination pattern of comprehensive legislative framework with significant implementation gaps, achieving a dimension score of 2.25, positioning between Aware (Level 2) and Developing (Level 3). The Digital Personal Data Protection Act (DPDPA) enacted in August 2023 establishes GDPR-equivalent data protection rights, including access, correction, deletion, and grievance mechanisms, with maximum penalties of up to 25 billion rupees (approximately $300 million USD). Constitutional foundation provides high-level legal protection through the Supreme Court's recognition of privacy as a fundamental right in Puttaswamy v. Union of India (2017).

Sectoral data localization enforcement has achieved significant effectiveness. The Reserve Bank of India's 2018 notification requires hard localization of payment system data and is supported by decisive enforcement actions: prohibiting American Express and Diners Club for 6 months due to non-compliance (2021), indefinitely banning Mastercard from new customer onboarding (2021). These actions demonstrate willingness to penalize major foreign companies and have triggered behavioral change, such as WhatsApp delaying UPI payment launch for three years (2017-2020) to achieve RBI compliance.

India has established world-leading Digital Public Infrastructure (DPI), with Aadhaar and India Stack creating efficiency value equivalent to 0.9% of GDP in 2022, projected to reach 2.9-4.2% by 2030. The National Data Access Platform (NDAP), India Urban Data Exchange (IUDX), and Account Aggregator Framework demonstrate operational data sharing infrastructure with actual economic impact. Domestic cloud infrastructure is expanding, with Reliance Jio (450 million customers, 2000MW AI capacity), Tata Communications (30% of global internet routing), and government MeghRaj cloud providing a certain sovereignty foundation.

However, the critical weakness is that DPDPA remains non-operational nearly two years after enactment. No Data Protection Board has been established, no enforcement actions have been taken, and implementation timelines (including the April 2025 target) have been repeatedly missed. This creates a fundamental gap between legislative achievement and operational data protection, keeping India at Level 2 (Aware) in data ownership legislation despite possessing comprehensive legal text. There is strategic tension between the loose general framework and strict sectoral requirements, with DPDPA adopting a blacklist approach allowing cross-border transfers (unless to notified countries), representing a retreat from the stricter requirements of the earlier 2019 draft. No blacklist has been published, no standard contractual clauses have been issued, and no adequacy determination procedures have been established, creating a dual system where payment and telecom data face hard localization while general data flows remain largely unrestricted.

Despite localization requirements, foreign cloud providers dominate the market, with AWS (32.6%), Azure (20.8%), and Google Cloud (11.4%) collectively controlling 65% of India's cloud market. Large-scale foreign cloud investments—Google's $15 billion over five years, Microsoft's $1.8 billion in Hyderabad, AWS's second India region—reinforce rather than reduce dependency. Localization compliance is often achieved through foreign providers building India data centers rather than shifting to domestic providers. Although India's policy framework strongly recognizes data as a "national asset" (2022 National Data Governance Framework, 2020 Non-Personal Data Framework), core regulatory and institutional mechanisms for data value capture are lacking. No accounting regulations allow data to be listed on balance sheets (Indian GAAP explicitly excludes it), zero recorded cases show companies listing data on balance sheets at asset value, and the government withdrew data monetization provisions in the 2022 policy after criticism. DPI creates efficiency value rather than data asset ownership value—this critical distinction limits India to Level 2 in data value inclusion.

Indicator Scores:

1.1 Legislation on data ownership: Level 2 - Aware

1.2 Domestic data storage: Level 3 - Developing

1.3 Protection of cross-border data transfers: Level 2 - Aware

1.4 Inclusion of data value for the public: Level 2 - Aware

Dimension 2: Digital Infrastructure Independence (2.75/5.0)

India's digital infrastructure independence reflects a contradictory position: possessing the world's largest IT services industry and substantial domestic capabilities in specific domains (fintech/payment software, cybersecurity), yet facing overwhelming foreign dependence in foundational hardware, operating systems, and most application software categories. The dimension score of 2.75 places it firmly in the Developing stage (Level 3).

Semiconductor investment and emerging manufacturing demonstrate India's most significant semiconductor manufacturing initiative in history, with $18.2 billion in projects approved since 2021, far exceeding the Level 3 threshold. The India Semiconductor Mission's $9.1 billion allocation demonstrates top-level policy commitment. Initial operational capacity is emerging, with Micron's ATMP facility (end of 2024/April 2025) and Tata's ATMP facility (mid-2025) achieving combined capacity of 91 million chips per day. India's first fab—the Tata-Powerchip collaboration ($11 billion, targeting 28nm production)—is proceeding on schedule, with delivery in December 2026 and technology transfer from Taiwan. A strong design ecosystem (150,000 engineers capable of 5nm ASIC design) and sixfold growth in electronics manufacturing ($21 billion to $125 billion, 2014-2024) provide a foundation for hardware independence trajectory.

Application software demonstrates excellence in the fintech domain. India has achieved world-class domestic capability through UPI, processing 85% of India's digital payments and 50% of global digital transaction volume, with 491 million users and 65 million merchants. UPI demonstrates international competitiveness, having been adopted by Japan, UAE, Singapore, and Nepal, with transaction volumes exceeding PayPal, Alipay, and PIX, and recognized by the IMF as a global benchmark. This proves India can develop internationally competitive application software when strategically focused and supported by strong government policy implementation, including ministerial directives, GeM procurement (13.43 trillion rupees in transactions), and India Software Product Registry. A large-scale software ecosystem (300,000+ entities, 160,000 government-recognized startups growing 40-fold since 2016) and a robust SaaS sector ($1.84 billion in funding over 9 months in 2025) demonstrate active development capabilities.

Cybersecurity capabilities and market show that India has established considerable information security capacity, with a domestic market valued at $4.04-6.87 billion in 2024, projected to reach $17.7 billion by 2033, far exceeding the Level 3 threshold. CERT-In demonstrates highly operational capabilities, handling over 1.6 million incidents annually, issuing 600+ alerts, and conducting 10,000 annual audits. Identifiable domestic companies include Quick Heal (30% domestic market share, operating in 80+ countries), major IT integrators (TCS, Wipro, Infosys, HCLTech), and specialized vendors like QNu Labs (quantum cryptography). India achieved Tier 1 status in the 2024 ITU Global Cybersecurity Index (98.49/100 points, ranked 10th globally, up from 47th), and successfully defended against massive DDoS attacks during the G20 Summit (1.6 million intrusion attempts per minute) demonstrating operational capabilities.

However, India currently depends on imports for 95% of semiconductors, with Taiwan alone supplying over 40%, creating geopolitical vulnerability. In foundational software, despite policy funding exceeding $270 billion, market outcomes show overwhelming foreign control across all categories: operating systems with Windows occupying 65.98% desktop share while domestic BOSS Linux remains under 1%; mobile operating systems with Android at 95.26%; cloud services with AWS, Azure, and Google collectively controlling 65%. Critically, the government's MeghRaj cloud certifies foreign CSPs (AWS, Azure, Google) as approved providers, undermining domestic preference. Databases are completely foreign-dominated (Oracle, MySQL, PostgreSQL), with zero identifiable Indian alternatives achieving significant market share. The middleware market is dominated by Oracle WebLogic, IBM WebSphere, and Red Hat JBoss. Domestic cloud provider market share is marginalized: Tata Communications approximately 3%, others (Netmagic, CtrlS) combined under 5%.

UPI's excellent success has not translated into independence in other application software categories. Office software has less than 1% domestic share (Microsoft/Google approximately 74% global control), search engines show Google's 97.75% monopoly with zero domestic alternatives, social media is dominated by Meta platforms, enterprise software is dominated by SAP/Oracle, and industrial software (CAD/EDA) is completely controlled by Siemens/Autodesk/Cadence.

Indicator Scores:

2.1 Independence of foundational hardware: Level 3 - Developing

2.2 Independence of foundational software: Level 2 - Aware

2.3 Independence of application software: Level 3 - Developing

2.4 Independence of information security: Level 3 - Developing

Dimension 3: Digital Governance Independence (3.5/5.0)

Digital Governance Independence is India's strongest dimension, scoring 3.5, positioning between Developing (Level 3) and Competent (Level 4), reflecting India's validated capabilities in legislating digital affairs, enforcing against major foreign tech companies, and meaningfully participating in international digital governance forums.

Legislative capacity reaches Level 4 (Competent), demonstrating strong capabilities in 5-6 of 7 key areas. India has enacted comprehensive digital governance legislation, including the 2023 DPDPA (GDPR-equivalent data protection), 2021 IT Intermediary Rules (platform regulation), and 2024 Digital Competition Bill (ex-ante regulation), despite opposition from the US-India Business Council and ITIF. Constitutional foundation (2017 Supreme Court privacy recognition) and validated ability to resist tech industry lobbying (in contrast to Brazil, where Google/Meta blocked fake news legislation for 4+ years) demonstrate legislative independence. Active antitrust enforcement through CCI, with fines of 1.338 billion rupees against Google (2022) and 213 million rupees against Meta (2024), shows willingness to penalize foreign giants. Telecommunications enforcement includes data breach fines against Airtel and Vodafone-Idea (5 million rupees each), and the financial sector sees RBI taking decisive action on payment violations.

Enforcement capacity reaches Level 3 (Developing), demonstrating active enforcement and documented behavioral change. Most notably, Twitter/X compliance rate increased from 11% to 100% (October 2022 to April 2023), achieved after Karnataka High Court enforcement and punitive fees. Comprehensive content blocking (36,838 URLs blocked 2018-2023, including 13,660 on X/Twitter, 7,502 accounts blocked in 2023 alone) and cybersecurity framework (2024 Tier 1 Global Cybersecurity Index status, 10th globally) demonstrate operational capabilities. However, only one documented behavioral change case (Twitter) meets the Level 3 minimum threshold, unable to reach Level 4 which requires multiple behavioral changes. DPDPA remains non-operational 18 months after enactment, with no Data Protection Board, creating a significant enforcement gap. CCI's digital market division has only 7 core staff responsible for entire digital market enforcement, facing "coordinated lobbying, behind-the-scenes pressure" from big tech companies.

In international rules leadership, India's most significant contribution is the DPI Stack framework (Aadhaar, UPI, DigiLocker), adopted by 12+ countries, endorsed by the G20 (2023), and incorporated into the UN Global Digital Compact. UPI processes 50% of global digital payment transaction volume, recognized by the IMF as a global benchmark, representing world-class innovation with international impact. India provides technical assistance to 30+ countries, co-leads the Global Partnership on AI (2024-2025), chairs the BRICS Digital Economy Working Group, demonstrating leadership capabilities. In technology standards, India actively participates in standards bodies: 5Gi integration in 3GPP, P-member status in 449 ISO committees, active participation in ITU-T and ITU-R, and over 18,000 members in IEEE. However, despite participation, India has zero declared standard-essential patents for 5G, compared to China's 33,000+ 5G SEPs. In behavioral rules, thematic focus is narrowly concentrated (DPI, digital payments, cybersecurity capacity building), with no participation in digital chapter negotiations of major trade agreements, and influence is primarily regional (South Asia, Southeast Asia, Africa) rather than global.

Indicator Scores:

3.1 Legislative capacity for digital affairs: Level 4 - Competent

3.2 Enforcement capacity for digital affairs: Level 3 - Developing

3.3 Leadership in international digital technology rules: Level 3 - Developing

3.4 Leadership in international digital behavior rules: Level 3 - Developing

Dimension 4: Digital Capability Independence (3.25/5.0)

Digital Capability Independence reflects a unique pattern: excellent scale in talent cultivation and strategic coordination, combined with critical weaknesses in technology commercialization and balanced industrial capabilities. The dimension score of 3.25 positions it between Developing (Level 3) and Competent (Level 4).

Talent cultivation reaches Level 4 (Competent), with India annually training 2.6 million STEM graduates, accounting for 31-34% of global STEM graduate output—the highest absolute number globally. Twenty-three IIT institutions represent world-class technical education, cultivating globally competitive graduates. Approximately 24,000 STEM doctoral degrees are awarded annually (4th globally), with 150+ institutions offering specialized AI/machine learning courses, demonstrating educational infrastructure scale. The IT industry employs 5.43 million workers (2024), with major companies (TCS 613,000, Infosys 318,000, Wipro 234,000 employees) providing an extensive on-the-job training ecosystem. However, 72.3% of US H-1B visas are issued to Indian nationals, representing massive talent drain to developed countries. Employability rate issues persist, with only 42-54% of engineering graduates considered employable by industry standards. Despite talent drain and quality concerns, India meets Level 4 quantitative thresholds: 1+ million STEM graduates annually (actual 2.6 million), 25%+ of global STEM output (actual 31-34%), world-class institutions (IITs), with quality metrics (rankings, employment) demonstrating international competitiveness.

Strategic coordination reaches Level 4 (Competent), demonstrated through sustained multi-decade planning spanning 40+ years. The Digital India Initiative ($13.5 billion budget) integrates nine pillars of infrastructure, governance, and services, supplemented by Atmanirbhar Bharat ($268 billion), IndiaAI Mission (103.72 billion rupees), and India Semiconductor Mission ($9.1 billion, total approved projects $18.2 billion), demonstrating comprehensive strategic framework. The digital economy contributes 11.74% of GDP (projected to reach 20% by 2026), DPI creates efficiency gains equivalent to 0.9% of GDP (projected to reach 2.9-4.2% by 2030), successful exports to 30+ countries, showing measurable integration with development. However, rural digital divide persists (70% poor connectivity), semiconductor dependence (90% imports, Level 3 only requires 50%) indicates incomplete integration.

Cutting-edge technology research and development reaches Level 3 (Developing), with 64,480 digital technology patents filed in 2023 (6th globally), a 15.7% year-over-year increase, with approximately 45% concentrated in ICT fields. AI research publications rank 5th globally, with significant contributions in machine learning, NLP, and computer vision. Major companies operate advanced R&D: TCS Innovation Labs ($1.6 billion), Infosys AI/automation focus, Wipro LabX, Reliance Jio indigenous 5G technology. However, R&D intensity at 0.64% of GDP (below the critical 1% threshold), with only $50 billion in absolute spending, compared to China's $723 billion—a 14-fold gap. Patent output (64,480) significantly lags behind China (1.6 million) and the US (350,000+).

Industry engineering capabilities reach Level 3 (Developing), with the IT industry overwhelmingly service-dominated, with services at $227 billion versus products at $43 billion (5.3:1 ratio), indicating limited product engineering depth. Export market concentration sees 54% directed toward the US, creating dependency vulnerability. Domestic product companies face scale challenges: the largest (Zoho $1 billion, Quick Heal $60 million) remain small compared to global giants.

Indicator Scores:

4.1 Cutting-edge technology research and development: Level 3 - Developing

4.2 Talent cultivation in universities: Level 4 - Competent

4.3 Industry engineering capabilities: Level 3 - Developing

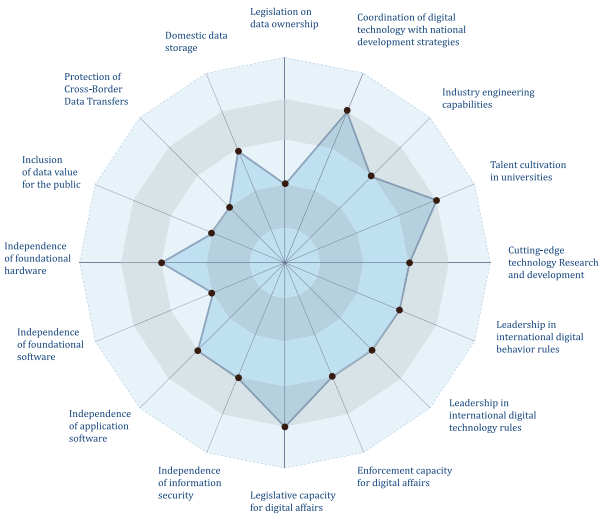
4.4 Coordination of digital technology with national development strategies: Level 4 - Competent

Summary

India's DSI score of 2.94 represents a nation actively developing digital sovereignty—surpassing the mere awareness stage, possessing operational capabilities and measurable progress in specific domains, but facing structural constraints, implementation gaps, and deployment challenges that prevent comprehensive independence. India's most unique challenge is the gap between capabilities and deployed sovereignty: the nation possesses excellent-scale talent production, substantial R&D activity, world-class service delivery, and validated governance capabilities, but these capabilities primarily flow toward integration with foreign-dominated systems rather than building domestic digital independence.

The capability-sovereignty paradox defines India's position. The capabilities of 5.43 million IT workers are deployed in serving foreign markets (59.3% service exports) rather than building domestic products. Seventy-two point three percent of 2.6 million annual STEM graduates drain to the US rather than remaining to build indigenous innovation. Comprehensive enacted legislation (DPDPA) delays implementation for 18 months, demonstrating policy-implementation gaps. Selective excellence exists in specific domains—UPI (85% domestic payments, 50% global volume), DPI framework (adopted by 12+ countries), IIT system (globally competitive education)—yet faces comprehensive foreign dependence at foundational layers: 95% semiconductor imports, 65% foreign cloud share, Google's 97.75% search monopoly, Microsoft/Google approximately 74% office software control.

India's digital sovereignty challenge lies primarily not in capability development—the nation has proven it can cultivate talent, conduct research, deliver world-class services, achieve excellent innovation (UPI), and enact comprehensive legislation. The challenge lies in converting these capabilities into deployed sovereignty: transforming service excellence into product independence, converting talent outflow into domestic retention, implementing enacted legislation in actual operational manner, extending sectoral success models (RBI payment data, UPI, IIT) to comprehensive domains, and redirecting capabilities toward building domestic infrastructure rather than serving foreign markets. India's digital sovereignty future depends less on developing new capabilities—these exist in abundance—and more on deploying existing capabilities for sovereignty rather than integration.



India's Digital Sovereignty Index Assessment Results

Dimension Average Scores:

- Dimension 1 - Data Ownership Independence: 2.25/5.0
- Dimension 2 - Digital Infrastructure Independence: 2.75/5.0
- Dimension 3 - Digital Governance Independence: 3.5/5.0
- Dimension 4 - Digital Capability Independence: 3.25/5.0

South Africa Digital Sovereignty Index Assessment

Assessment Date: October 15, 2025, **DSI Overall Score**: 1.94/5.0 **Country Code**: ZA

Overview

South Africa scores 1.94 out of 5 in the Digital Sovereignty Index assessment, presenting digital sovereignty characteristics marked by a severe asymmetry between legislative maturity and implementation capacity. The country demonstrates developing-level performance in the Data Ownership Independence and Digital Governance Independence dimensions (both scoring 2.25), showcasing its policy-making advantages through comprehensive legislation such as the Protection of Personal Information Act (POPIA) and active parliamentary engagement. Legislative capacity reaches Level 3 (Developing), with POPIA comparable to GDPR, and the Information Regulator handling 982 complaints and implementing its first monetary penalties in the 2023-2024 fiscal year (R5 million each to government departments).

However, Digital Infrastructure Independence (1.50) and Digital Capability Independence (1.75) remain in the initial or aware stages, revealing the country's fundamental dependence on foreign platforms, hardware, and software across all layers of the technology stack. South Africa has no semiconductor manufacturing capacity, no domestic operating system or database platform development, minimal application software independence, and near-complete dependence on foreign information security technologies. R&D investment at 0.85% of GDP (below the global 1.7%), patent output representing only 0.06% of global share, and brain drain with over 900,000 South African citizens residing abroad further erode technical capabilities. The 10-year delay from POPIA's enactment (2013) to first penalties (2023), maximum penalties of R10 million (approximately $550,000) offering insufficient deterrence to multinational tech companies, and the Information Regulator's approximately 100 staff members handling nearly a thousand annual complaints exemplify South Africa's systemic challenges in translating legislation into operational capability.

Dimension 1: Data Ownership Independence (2.25/5.0)

South Africa's data governance demonstrates characteristics of legislative sophistication but limited enforcement, with a dimension score of 2.25. The Protection of Personal Information Act (POPIA) was enacted in 2013 and fully implemented in 2020-2021, establishing a comprehensive data protection framework comparable to GDPR, with constitutional grounding in Section 14 privacy rights of the 1996 Constitution. Eight data protection principles include lawfulness, purpose limitation, minimization, quality, openness, security safeguards, data subject participation, and accountability, corresponding to GDPR's core principles. Data subject rights include access, correction, deletion, and objection to processing, with maximum penalties of R10 million (approximately $550,000) or 0.5% of annual turnover, whichever is higher.

The Information Regulator, as an independent enforcement agency, has been in full operation since 2021, handling 982 complaints in the 2023-2024 fiscal year with a resolution rate of 68.8%. In 2023, it implemented its first monetary penalties, fining the Department of Justice and the Department of Basic Education R5 million each. While these penalties targeted government entities, they demonstrate the regulator's willingness to exercise punitive authority. Regarding data localization, the National Data and Cloud Policy passed in 2024 requires government data involving national security to be stored within South Africa's borders, with cloud service providers required to register in South Africa and comply with POPIA. Cross-border data transfers are regulated through Section 72 of POPIA, requiring destination countries to have adequate protection levels or alternative safeguard measures.

However, enforcement capacity faces significant constraints. Maximum penalties of R10 million are far below GDPR levels (20 million euros or 4% of global revenue), offering insufficient deterrence to multinational tech companies with revenues measured in billions of dollars. Incidents such as WhatsApp challenging the regulator's jurisdiction and Meta/Google/X initially refusing information requests highlight the power asymmetry between South Africa and foreign technology platforms. Approximately 100 staff members handling nearly a thousand annual complaints represents severely inadequate resource allocation. The 10-year delay from legislative enactment (2013) to first penalties (2023) demonstrates the implementation gap. While data localization requirements exist, they are limited in practical application due to the lack of published adequacy decisions and systematic monitoring capabilities. Regarding public data value, while recognizing data value through the 2020 Open Data Policy and Digital Economy Masterplan, there is a lack of systematic value capture mechanisms, data dividend schemes, or commercialization frameworks.

Indicator Scores:

1.1 Legislation on data ownership: Level 3 - Developing

1.2 Domestic data storage: Level 2 - Aware

1.3 Protection of cross-border data transfers: Level 2 - Aware

1.4 Inclusion of data value for the public: Level 2 - Aware

Dimension 2: Digital Infrastructure Independence (1.50/5.0)

Digital infrastructure is South Africa's weakest dimension, with an average score of 1.50, demonstrating near-complete dependence on external sources. Both foundational hardware and foundational software receive Level 1 (Initial), revealing the deepest structural vulnerabilities. South Africa has no semiconductor manufacturing capacity, no significant server production industry, and produces no core computing hardware components. The digital technology sector primarily serves as a distribution and integration center for the African market rather than as a production center. The entire supply chain from semiconductors and processors to servers and storage systems is completely controlled by foreign entities, creating strategic vulnerabilities.

In foundational software, South Africa's digital infrastructure operates almost entirely on foreign platforms. There is a lack of indigenous operating system development, with government and private systems primarily based on Microsoft Windows, various Linux distributions, and other foreign platforms. Database systems used are overwhelmingly foreign products,

including Oracle, Microsoft SQL Server, MySQL, and PostgreSQL, with no significant indigenous database platform development. Regarding cloud platform software, organizations heavily rely on foreign cloud infrastructure such as AWS, Microsoft Azure, and Google Cloud Platform. Even though the 2024 National Data and Cloud Policy requires certain government data to be stored domestically, the software platforms managing this data remain owned and controlled by foreign companies. There is no indigenous cloud platform development and no significant middleware product development.

The application software domain demonstrates moderate indigenous development capacity (Level 2). Local companies like Yoco and SnapScan have developed successful application platforms serving the South African market, indicating some indigenous application development capability. Universities train software engineering graduates, and startup ecosystems focused on developing applications for the African market are emerging in Cape Town and Johannesburg. However, critical enterprise and productivity applications remain dominated by foreign platforms. Microsoft Office and Google Workspace hold overwhelming dominance in government, business, and education sectors, while enterprise resource planning systems are primarily SAP, Oracle, and Microsoft Dynamics. Despite developing local mobile applications, these applications operate almost entirely on Android and iOS, representing integration into foreign ecosystems rather than independent alternatives.

Information security reaches Level 2 (Aware), establishing a foundational framework through the 2020 Cybercrimes Act and National Cybersecurity Policy Framework, indicating recognition of information security importance. The National Cybersecurity Hub provides incident response and coordination. However, information security capabilities depend overwhelmingly on foreign security technologies. Cybersecurity software deployed in government and private systems—including antivirus platforms, intrusion detection systems, SIEM tools, and encryption systems—comes almost entirely from international companies such as Symantec, McAfee, Palo Alto Networks, and Cisco. The lack of indigenous encryption technologies and security chip production creates special vulnerabilities.

Indicator Scores:

2.1 Independence of foundational hardware: Level 1 - Initial

2.2 Independence of foundational software: Level 1 - Initial

2.3 Independence of application software: Level 2 - Aware

2.4 Independence of information security: Level 2 - Aware

Dimension 3: Digital Governance Independence (2.25/5.0)

The Digital Governance Independence dimension scores 2.25, demonstrating significant asymmetry between legislative capacity and enforcement capacity. Legislative capacity reaches Level 3 (Developing), with the South African parliament demonstrating active engagement capability in digital governance issues through a comprehensive legal framework covering data protection, cybersecurity, electronic transactions, and digital economy development. The 2013 POPIA, 2020 Cybercrimes Act, and 2002 Electronic Communications and Transactions Act (ECTA) constitute a multi-layered legislative framework. The formulation of the Digital Economy Masterplan and ongoing policy initiatives such as the National Data and Cloud Policy (2024) indicate parliament's continued attention to emerging digital governance challenges. Parliamentary committees holding hearings on platform regulation, artificial intelligence governance, and digital economy competitiveness indicate government recognition that digital technology requires coordinated legislative and policy responses.

However, a significant gap exists between legislative enactment and operational implementation. The 7-8 year delay from POPIA's enactment in 2013 to full implementation in 2021 exemplifies this pattern: legislative capacity to draft and pass advanced laws exceeds institutional capacity to implement these laws. While cybersecurity legislation exists, implementation of the National Cybersecurity Policy Framework faces resource constraints and inter-agency coordination challenges. Certain digital governance areas, despite growing importance, still lack comprehensive legisla-

tion, such as platform regulation, artificial intelligence governance, content moderation, and algorithmic accountability.

Enforcement capacity reaches Level 2 (Aware), with South Africa establishing digital affairs enforcement agencies, most notably the Information Regulator responsible for enforcing POPIA and PAIA. The regulator began operations in 2021, with complaint volumes increasing annually to 982 in the 2023-2024 fiscal year, with a resolution rate of 68.8%. In 2023, it implemented its first monetary penalties, fining government departments R5 million each for data protection violations. However, severe resource constraints fundamentally limit enforcement effectiveness. Approximately 100 staff members responsible for enforcing data protection and information access legislation across a population of 60 million and thousands of organizations is far from adequate for comprehensive enforcement. The R10 million (approximately $550,000) penalty cap offers insufficient deterrence to large tech companies with revenues in the billions of dollars. WhatsApp challenging jurisdiction and Meta/Google/X initially refusing information requests demonstrate power asymmetry.

Regarding leadership in international rules, South Africa participates in international digital technology standard-setting organizations and contributes to regional digital governance frameworks, particularly within the African Union. The country holds membership in standards organizations such as ISO and ITU. However, South Africa's influence on global technology standards remains limited by structural factors including technical capability gaps, resource constraints, and power asymmetry with major technology-producing nations. South Africa has no major technology standard adopted internationally. Regional leadership represents South Africa's primary area of influence in digital technology governance, with South Africa playing an active role in African Union digital initiatives, contributing to the development of continental data protection frameworks. Regarding international digital behavior rules, South Africa participates in multilateral processes such as UN cybersecurity discussions and African Union digital governance initiatives, supporting approaches emphasizing multilateralism and developing country solidarity, but actual influence on global digital behavior rules remains limited.

Indicator Scores:

3.1 Legislative capacity for digital affairs: Level 3 - Developing

3.2 Enforcement capacity for digital affairs: Level 2 - Aware

3.3 Leadership in international digital technology rules: Level 2 - Aware

3.4 Leadership in international digital behavior rules: Level 2 - Aware

Dimension 4: Digital Capability Independence (1.75/5.0)

The Digital Capability Independence dimension scores 1.75, with three of four indicators at Level 2 (Aware) and one at Level 1 (Initial), revealing severe constraints on capability building. Cutting-edge technology research and development reaches Level 2 but faces major limitations. R&D spending accounts for approximately 0.85% of GDP, significantly below the global average of 1.7%, and far below leading innovation economies such as Israel (5.6%), South Korea (4.8%), or China (2.4%). This limited investment constrains the country's ability to conduct cutting-edge research in key digital technologies such as AI, semiconductor technology, quantum computing, and advanced networking. Patent output provides a quantitative measure of innovation capacity, with South Africa accounting for approximately 0.06% of global patents, with minimal patent activity in cutting-edge digital technology fields such as AI, machine learning, semiconductor design, and advanced telecommunications.

Severe brain drain erodes research capability building. Over 900,000 South African citizens reside abroad, many with advanced technical education backgrounds. Technically skilled researchers and engineers emigrate to high-paying positions in the United States, United Kingdom, and Australia, where research funding, infrastructure, and career opportunities exceed what South African institutions can provide. This brain drain means that even when South African universities train capable researchers, retention becomes problematic.

Talent cultivation in universities reaches Level 2 (Aware), with South Africa having multiple universi-

ties offering computer science, electrical engineering, and related technical disciplines. Institutions such as the University of Cape Town, University of the Witwatersrand, and Stellenbosch University provide undergraduate and graduate degrees in computer science, information technology, and engineering disciplines. Some programs receive international recognition, with graduates entering global tech companies and research institutions. However, the scale of technical education relative to industry needs and national development needs remains insufficient. STEM enrollment rates are constrained by limited university capacity, infrastructure challenges including electricity supply interruptions, and high dropout rates in demanding technical disciplines. Mismatches between educational output and industry needs are reflected in persistent talent shortages. Resource constraints affect education quality and infrastructure, with universities facing funding limitations that constrain laboratory facilities, computing infrastructure, research opportunities, and faculty compensation.

Industry engineering capabilities receive Level 1 (Initial), the lowest score in this dimension. South Africa demonstrates minimal capability in the digital technology field. The country has no semiconductor manufacturing, hardware production limited to system integration, software development concentrated in applications rather than platforms, and ongoing engineering talent drain. The local technology sector primarily operates as a regional service and integration center rather than as a producer of foundational digital technologies. South African software companies create mobile applications, business software, and sector-specific solutions, typically based on Android, iOS, cloud platforms, or enterprise software frameworks developed by foreign companies. This integration into foreign ecosystems, while demonstrating technical capability, perpetuates dependence at the platform level.

Strategic coordination reaches Level 2 (Aware), with South Africa formulating comprehensive strategic frameworks, most notably the Digital Economy Masterplan, establishment of the Fourth Industrial Revolution Commission, and the National Data and Cloud Policy passed in 2024. These strategic documents and institutions indicate government recognition that digital technology is a critical factor for national development requiring coordinated policy attention. However, significant gaps exist between strategy formulation and implementation. Resource constraints limit the government's ability to fund strategic initiatives. Cross-agency coordination, despite institutional frameworks such as the Fourth Industrial Revolution Commission, still faces practical challenges. Infrastructure challenges fundamentally undermine digital strategies, with unstable electricity supply directly contradicting the digital economy vision that assumes reliable power.

Indicator Scores:

4.1 Cutting-edge technology research and development: Level 2 - Aware

4.2 Talent cultivation in universities: Level 2 - Aware

4.3 Industry engineering capabilities: Level 1 - Initial

4.4 Coordination of digital technology with national development strategies: Level 2 - Aware

Summary

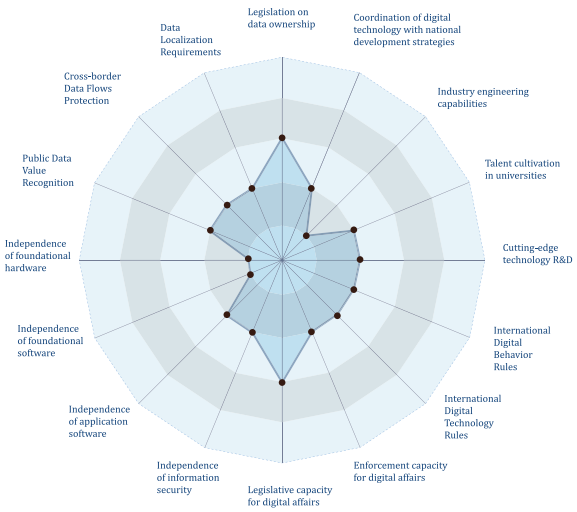
South Africa presents a digital sovereignty development model characterized by advanced legislation but severely limited execution and infrastructure. The overall DSI score of 1.94 reflects extremely unbalanced development across four dimensions: Data Ownership Independence and Digital Governance Independence reach developing levels, while Digital Infrastructure Independence and Digital Capability Independence remain in initial or aware stages. The most notable pattern is the persistent gap between legislative or policy sophistication and operational execution capacity, as well as the deepest digital sovereignty vulnerabilities revealed in the infrastructure dimension.

South Africa is capable of formulating legislation comparable to international standards—POPIA is comparable to GDPR, the Cybercrimes Act addresses digital security threats, and strategic documents articulate advanced digital transformation visions. However, enforcement capacity is severely constrained by limited resources, insufficient penalty caps (R10 million versus GDPR's 20 million euros), and jurisdictional challenges with foreign technology companies. The Information Regulator's approximately 100 staff members handling

nearly a thousand annual complaints, and the 10-year delay from POPIA's enactment (2013) to first penalties (2023), fully illustrate how resource and capacity constraints prevent even well-designed legislation from operating effectively for extended periods.

The infrastructure dimension reveals South Africa's deepest digital sovereignty vulnerabilities. All four infrastructure indicators demonstrate minimal indigenous capabilities, creating structural dependencies at every layer of the technology stack. South Africa has no semiconductor manufacturing, no indigenous operating system or database platform development, and almost complete dependence on foreign security technologies. This infrastructure dependence fundamentally constrains all other dimensions: data sovereignty visions must be built on storage systems controlled by foreign companies, digital governance enforcement must use monitoring tools developed abroad, and capability development occurs within technology ecosystems designed and controlled by foreign entities. Resource constraints appear in 11 of the 16 indicators, representing the most consistent cross-domain limitation. Brain drain (over 900,000 South Africans abroad), limited R&D funding (0.85% of GDP), minimal patent output (0.06% global share), and infrastructure challenges including unstable electricity supply all stem from or are exacerbated by resource scarcity.

The fundamental insight from South Africa's digital sovereignty assessment is that regulatory sophistication without corresponding infrastructure, capability, and enforcement capacity support creates an illusion of sovereignty rather than substance. South Africa can enact legislation comparable to GDPR, establish independent regulatory agencies, and articulate advanced digital strategies, but until these frameworks are built on indigenous infrastructure, enforced by well-resourced agencies with meaningful punitive authority, and supported by an indigenous technology industry capable of providing alternatives to foreign platforms, digital sovereignty remains vision rather than reality.



South Africa Digital Sovereignty Index Assessment Results

Dimension Average Scores:

- Dimension 1 - Data Ownership Independence: 2.25/5.0
- Dimension 2 - Digital Infrastructure Independence: 1.50/5.0
- Dimension 3 - Digital Governance Independence: 2.25/5.0
- Dimension 4 - Digital Capability Independence: 1.75/5.0

United Arab Emirates Digital Sovereignty Index Assessment

Assessment Date: October 15, 2025, **DSI Overall Score**: 2.38/5.0 **Country Code**: AE

Overview

The United Arab Emirates achieved a score of 2.38 out of 5 in the Digital Sovereignty Index assessment, presenting a unique positioning as a "sophisticated digital intermediary" rather than pursuing complete technological autonomy. The country has decisively moved beyond the initial awareness stage, implementing world-class digital strategies in targeted areas, with Digital Capability Independence reaching 3.0 (Developing). Strategic coordination capability reaches Level 4 (Competent), evidenced by over 15 years of continuous planning, globally pioneering institutional innovations (world's first AI Minister in 2017), and comprehensive implementation (Mars mission, 25 billion dirham digital investment). STEM gender equality reaches Level 3, with female STEM graduates accounting for 56-61% (highest globally, compared to 35% global average), and infrastructure deployment is world-leading, with 5G median speeds of 557.63 Mbps and population coverage of 98.5%.

However, the country faces structural constraints of small developed nations. A small-scale population (approximately 10 million total population, approximately 1 million citizens) results in limited data collection (Indicator 1.1 Level 2), R&D output accounting for less than 0.5% globally (Indicator 4.1 Level 2), and moderate engineering workforce scale (Indicator 4.3 Level 3). Technology dependence permeates hardware (US semiconductors, Microsoft Azure for "sovereign" cloud), software (OpenAI models, foreign platforms holding over 55% market share), and standards (limited international influence). Talent dependence is reflected in 92% expatriate workforce, which despite impressive aggregate statistics creates long-term sovereignty vulnerabilities. International rule-making influence is limited (Dimension 3 average 2.25) — a sophisticated participant and convener but not a rule-maker.

Dimension 1: Data Ownership Independence (2.00/5.0)

The UAE's data resource independence demonstrates sophisticated governance but limited scale characteristics, with a dimension score of 2.00. Legislation on data ownership reaches Level 2 (Aware), with the 2021 Federal Data Protection Law (FDPL) establishing a modern data protection framework covering data subject rights, data controller obligations, and cross-border transfer rules. The Office of Data Protection (ODP) was established in 2022 as an enforcement agency, demonstrating institutionalized commitment. The Abu Dhabi Global Market (ADGM) and Dubai International Financial Centre (DIFC) maintain independent data protection regimes, creating a multi-layered regulatory environment.

Domestic data storage reaches Level 3 (Developing), the strongest indicator in this dimension. The 2019 Critical Data Regulation stipulates that government and critical sector data must be stored within the UAE, enforced by UAE-IX (UAE Internet Exchange) and TDRA (Telecommunications and Digital Government Regulatory Authority). Cloud service providers have established local data centers to comply with requirements, including AWS, Microsoft Azure, Oracle, and Alibaba Cloud facilities in the UAE. However, these are local deployments of foreign cloud providers rather than indigenous platforms, representing compliance rather than true sovereignty.

Protection of cross-border data transfers reaches only Level 1 (Initial), the only Level 1 indicator in the assessment, reflecting an incomplete framework. The FDPL allows transfers when appropriate safeguards are met, but lacks published adequacy decisions, standard contractual clauses, or detailed implementation guidelines, creating regulatory uncertainty. The small-scale population fundamentally limits the UAE's leverage in negotiating data transfer agreements, with large tech companies effectively setting terms for UAE market access.

Inclusion of data value for the public reaches Level 2 (Aware), with policy recognition but limited operations. National strategies including "Smart Dubai 2021" and the AI Strategy identify data as an economic asset. However, there is a lack of systematic data dividend programs, public data monetization frameworks, or measurable mechanisms for redistributing data value to the public. Government open data initiatives exist but primarily focus on efficiency rather than value capture.

Indicator Scores:

1.1 Legislation on data ownership: Level 2 - Aware

1.2 Domestic data storage: Level 3 - Developing

1.3 Protection of cross-border data transfers: Level 1 - Initial

1.4 Inclusion of data value for the public: Level 2 - Aware

Dimension 2: Digital Infrastructure Independence (2.25/5.0)

Digital infrastructure independence demonstrates world-class deployment coexisting with foreign dependence, with a dimension score of 2.25. Independence of foundational hardware reaches Level 2 (Aware), with the UAE having no semiconductor manufacturing capability, completely reliant on imported chips (primarily from the US, Taiwan, South Korea). Although GLOBALFOUNDRIES has a fab in Abu Dhabi (acquired in 2009), this is a foreign-owned operation (US company), representing foreign direct investment rather than indigenous capability. Servers and network equipment are procured from international suppliers including Cisco, Huawei, Dell, HP, with no significant domestic hardware manufacturing ecosystem.

Independence of foundational software similarly reaches Level 2 (Aware), with systems running on foreign platforms. The operating system market is entirely dominated by Microsoft Windows (approximately 73% desktop), macOS, iOS, and Android, with no indigenous operating system development. Database systems are primarily Oracle, Microsoft SQL Server, MySQL, and PostgreSQL, with no identifiable UAE indigenous database platforms. Regarding cloud platforms, although the "UAE Sovereign Cloud" was launched in 2023, this is a joint venture based on Microsoft Azure technology

(G42+Microsoft), representing local deployment of foreign technology rather than an indigenous platform. Middleware systems rely on Oracle Fusion, IBM products, and Microsoft technologies, with no indigenous middleware development.

Independence of application software reaches Level 2 (Aware), with local development existing but limited. E-government platforms represent indigenous application capabilities, including UAEPASS (digital identity), Smart Dubai applications, and Abu Dhabi government services. The fintech sector is active, but local companies primarily serve as systems integrators rather than platform developers. Office productivity software is entirely dominated by Microsoft Office (approximately 55%) and Google Workspace, with no indigenous alternatives. Social media, search, and enterprise software are completely controlled by foreign platforms.

Independence of information security reaches Level 3 (Developing), the strongest indicator in this dimension. The 2019 National Cybersecurity Strategy and Electronic Crimes Law establish a comprehensive framework, with the UAE Cybersecurity Council (CSC) coordinating national cybersecurity efforts. Post-quantum encryption capabilities through TDRA and Etisalat investments demonstrate advanced awareness. However, deployed security technologies primarily come from foreign suppliers: Palo Alto Networks, Cisco, Fortinet, Symantec. Local companies like DarkMatter provide consulting and integration, but rely on foreign core technologies.

Indicator Scores:

2.1 Independence of foundational hardware: Level 2 - Aware

2.2 Independence of foundational software: Level 2 - Aware

2.3 Independence of application software: Level 2 - Aware

2.4 Independence of information security: Level 3 - Developing

Dimension 3: Digital Governance Independence (2.25/5.0)

Digital governance independence demonstrates strong domestic frameworks but limited international influence, with a dimension score of 2.25. Legislative capacity for digital affairs reaches Level 3 (Developing), with the UAE establishing a comprehensive digital governance legal framework including the 2021 FDPL, 2019 Critical Data Regulation, 2012 Cybercrime Law (revised 2021), and 2024 AI Charter. The multi-layered regulatory structure demonstrates sophistication through federal laws, ADGM/DIFC independent regimes, and industry-specific regulations. Legislative speed is rapid — the FDPL took only 18 months from draft to enactment, and the AI Charter was launched less than 18 months after ChatGPT's release, demonstrating agility.

Enforcement capacity for digital affairs reaches Level 2 (Aware), with institutions established but limited track record. The Office of Data Protection (ODP) was established in 2022, but as of October 2025 there are no publicly recorded data protection violation fines or enforcement actions. Cybercrime Law enforcement primarily targets traditional crimes (financial fraud, identity theft) rather than digital sovereignty-related violations (unauthorized data transfers, platform non-compliance). The lack of public enforcement cases may reflect compliance or reflect reluctance to enforce against large foreign tech companies.

Leadership in international digital technology rules reaches Level 2 (Aware), with active participation but limited influence. The UAE holds memberships in standards organizations including ISO, ITU, IEEE, participating through TDRA and the Emirates Authority for Standardization and Metrology (ESMA). However, there are no identifiable major UAE technical standards achieving international adoption. Participation primarily involves implementing international standards (ISO 27001, ITU recommendations) rather than formulating new standards. The small-scale technology industry limits the generation of standards-essential patents, thereby limiting standards-setting influence.

Leadership in international digital behavior rules reaches Level 2 (Aware), with sophisticated dialogue but limited rule-making. The UAE serves as a global dialogue convener for events such as the AI Action

Summit (2024), demonstrating convening capabilities. UN virtual worlds co-leadership (with Japan, 2024) represents emerging governance leadership. However, there is a lack of identifiable UAE-initiated digital behavior rules achieving international adoption. Digital governance positions typically align with US or EU frameworks rather than independent alternatives. Participation in UN, ITU, and GCC forums demonstrates activity but primarily as a participant rather than a rule-shaper.

Indicator Scores:

3.1 Legislative capacity for digital affairs: Level 3 - Developing

3.2 Enforcement capacity for digital affairs: Level 2 - Aware

3.3 Leadership in international digital technology rules: Level 2 - Aware

3.4 Leadership in international digital behavior rules: Level 2 - Aware

Dimension 4: Digital Capability Independence (3.00/5.0)

Digital Capability Independence is the UAE's strongest dimension, scoring 3.00, demonstrating strategic excellence but scale constraints. Cutting-edge technology research and development reaches Level 2 (Aware), with R&D investment at approximately 1.3% of GDP (2023), a moderate level but limited in total volume due to small economic scale. Patent output is minimal, accounting for less than 0.5% of the global total, primarily concentrated in smart cities, AI applications, and clean energy rather than core digital technologies. The Mohamed bin Zayed University of Artificial Intelligence (MBZUAI) and Dubai Future Foundation represent institutionalized R&D commitment, but absolute output is mathematically limited by population scale. International collaborations (with MIT, Carnegie Mellon) provide capability access, but represent technology transfer rather than indigenous innovation leadership.

Talent cultivation in universities reaches Level 3 (Developing), demonstrating unique strengths and constraints. Female STEM graduates account for 56-61%, the highest globally compared to the 35% global average, representing outstanding gender equality achievement. However, 92% expatriate workforce creates sovereignty vulnerability — talent scale is impressive but non-permanent, potentially lost with economic or policy changes. Universities including MBZUAI, Khalifa University, and UAE University provide STEM education, but total graduate numbers are limited due to small population. Education quality is enhanced through international collaborations (NYU Abu Dhabi, Sorbonne Paris), but these represent foreign university branches rather than indigenous institutions.

Industry engineering capabilities reach Level 3 (Developing), moderate scale with systems integration specialization. The technology sector employs approximately 200,000-250,000 workers (approximately 2-2.5% of workforce), mostly expatriates. Local companies such as G42, DarkMatter, Careem (acquired by Uber) demonstrate engineering capabilities, but primarily at the application layer rather than platforms or infrastructure. Systems integration and customization are core strengths — deploying and adapting foreign technologies for local needs (smart cities, e-government). Software development exists but is concentrated in mobile applications, government services, and fintech integration, rather than operating systems, databases, or cloud platform development.

Coordination of digital technology with national development strategies reaches Level 4 (Competent), one of only two Level 4 indicators in the entire assessment, representing the UAE's most significant advantage. Over 15 years of continuous strategic planning spans regime transitions, including Vision 2021 (2010), AI Strategy 2031 (2017), Mars 2117 Strategy (2017). World-first institutional innovations include the world's first AI Minister in 2017, Minister of State for AI and Virtual Reality in 2019, and Advanced Technology and Space Agency in 2020. Implementation track record is strong: successful Mars mission (Hope probe, 2021), 25 billion dirham digital investment, Expo 2020 digital showcase. Cross-agency coordination is achieved through the Prime Minister's Office Digital Government, Smart Dubai Office, and emirate-level digital agencies. Integration spans economic (free zones, entrepreneurship support), social (digital literacy), and strategic (defense, space) sectors, demonstrating comprehensiveness.

Indicator Scores:

4.1 Cutting-edge technology research and development: Level 2 - Aware

4.2 Talent cultivation in universities: Level 3 - Developing

4.3 Industry engineering capabilities: Level 3 - Developing

4.4 Coordination of digital technology with national development strategies: Level 4 - Competent

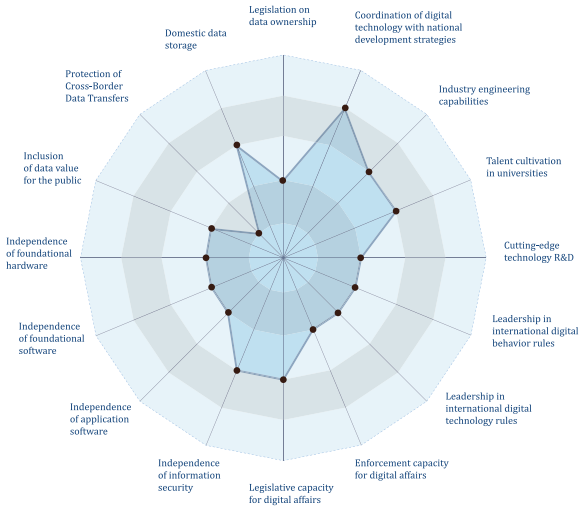
Summary

The UAE's DSI score of 2.38 represents a "sophisticated digital intermediary" model, a rational strategy for small wealthy nations seeking influence and economic benefits without shouldering the geopolitical burden of technological autonomy. The country has decisively moved beyond initial awareness, implementing world-class capabilities in targeted areas, but faces structural constraints that policy cannot overcome. Small-scale population creates mathematical limits in data scale, R&D output, and workforce, regardless of investment levels. The UAE faces a 3-4 level strategic ceiling, but proves that small developed nations can achieve significant digital capabilities and global influence in specialized areas.

The UAE's unique approach is embodied in a four-fold intermediary positioning: geographic intermediary (balancing US and Chinese technology ecosystems), regulatory intermediary (combining business openness with security controls), technology intermediary (deploying and integrating foreign technologies rather than developing complete indigenous stacks), and knowledge intermediary (attracting global talent rather than relying purely on domestic capabilities). This is not a failure of independence but a deliberate optimization for quality and specialization rather than scale and completeness.

The UAE's most significant strength is strategic coordination (Level 4), evidenced by over 15 years of continuous planning, world-first institutional innovations (world's first AI Minister), and comprehensive implementation (Mars mission, 25 billion dirham investment). STEM gender equality (56-61% female, highest globally) and infrastructure deployment (557.63 Mbps 5G speeds, 98.5% coverage) demonstrate excellence in targeted areas. However, 92% expatriate workforce creates talent dependence, technology dependence permeates hardware (no semiconductor manufacturing), software (foreign platforms holding over 55% market share), and standards (limited international influence), and limited enforcement track record (ODP has no public fine records) demonstrates implementation gaps.

The future trajectory is likely continued niche specialization strengthening (AI applications, cybersecurity, smart city technologies), with selected indicators potentially reaching Level 4 (UN virtual worlds co-leadership, continued STEM talent growth), but scale limitations will continue to constrain overall independence in data, R&D, and workforce. The intermediary role as core strategy will likely continue, positioning the UAE as a regional digital hub rather than a comprehensive technology power.



UAE Digital Sovereignty Index Assessment Results

Dimension Average Scores:

- Dimension 1 - Data Ownership Independence: 2.00/5.0
- Dimension 2 - Digital Infrastructure Independence: 2.25/5.0
- Dimension 3 - Digital Governance Independence: 2.25/5.0
- Dimension 4 - Digital Capability Independence: 3.00/5.0

Egypt Digital Sovereignty Index Assessment

Assessment Date: October 15, 2025 **DSI Total Score**: 1.94/5.0 **Country Code**: EG

Overview

Egypt scores 1.94 out of 5.0 in the Digital Sovereignty Index assessment, presenting a distinctive characteristic of "framework sovereignty rather than operational sovereignty." The country has established comprehensive legal frameworks and strategic planning, including GDPR-inspired comprehensive data protection legislation, a National AI Strategy and Vision 2030, with legislative capacity reaching Level 3 (Developing) and strategic coordination reaching Level 3. Egypt demonstrates genuine capabilities in specific areas—the most mature fabless semiconductor design ecosystem in the MENA region, prominent fintech and educational software applications, first-tier ranking in the Global Cybersecurity Index (100/100 points), and annual production of approximately 207,000 STEM graduates.

However, systematic implementation gaps and structural dependencies prevent intentions from translating into actual capabilities. The Personal Data Protection Center remains non-operational four years after legislative authorization, making citizens' data protection rights effectively unenforceable, with zero foreign tech platforms changing behavior due to Egyptian enforcement. The 86.5% STEM graduate emigration rate severely undermines capability-building investments, making Egypt a STEM training provider for destination countries rather than a builder of domestic capacity. Complete dependence on Microsoft, AWS, Oracle, SAP, and other foundational software, with government strategic partnerships further deepening dependencies. IT exports are 92% services rather than products, with 240,000 IT professionals creating $6.2 billion in exports but serving foreign companies rather than building domestic technological independence. Annual patent output of 881-1,027 (only 2-5% of the Level 3 threshold), R&D investment at 1.02% of GDP (below the 1.5% threshold), with the private sector accounting for only 2.7%.

Dimension 1: Data Ownership Independence (1.75/5.0)

Egyptian data governance displays comprehensive legislative frameworks but fundamental implementation obstacles, with a dimension average of 1.75. Legislation on data ownership reaches Level 2 (Aware), with the 2020 Personal Data Protection Law (Law No. 151) establishing a GDPR-inspired comprehensive framework covering data subject rights (access, correction, deletion, restriction of processing, portability), data controller obligations, and cross-border transfer rules. The law mandates the establishment of the Personal Data Protection Center as an independent regulatory authority with inspection, investigation, and penalty powers. However, this center remains non-operational more than four years after the law's promulgation, with implementing regulations delayed by 3.5 years, creating a fundamental barrier between legal frameworks and actual implementation.

Domestic data storage reaches Level 2 (Aware), with the government data localization project achieving concrete results by successfully migrating 114 government entities to domestic data centers (120PB capacity), demonstrating Egypt's implementation capability. Prime Ministerial Decree No. 266 of 2020 requires government data to be stored within Egyptian territory. However, this capability has not extended to the broader data protection field. Private sector and citizen data protection frameworks are effectively non-existent due to the non-operation of the Personal Data Protection Center, with foreign cloud providers dominating the market (AWS, Microsoft Azure, Oracle) without needing to comply with localization requirements.

Protection of cross-border data transfers reaches only Level 1 (Initial), the lowest indicator in this dimension. Articles 26-27 of the Personal Data Protection Law establish detailed cross-border transfer rules, requiring adequacy decisions or standard contract clauses, and prohibiting transfers to countries that do not provide adequate protection. However, due to the non-operation of the Personal Data Protection Center, these provisions are completely unimplemented—zero adequacy decisions issued, no standard contract clauses approved, no licensing system in operation. Data flows freely across borders without any sovereign protection.

Inclusion of data value for the public reaches Level 2 (Aware), with strategic recognition of data value but lack of economic mechanisms. Vision 2030 (2016) identifies data as a strategic resource, the National AI Strategy 2019 emphasizes a data-driven economy, and government open data initiatives demonstrate awareness of data as a public asset. However, there is a lack of systematic data value capture mechanisms, data dividend programs, or regulatory frameworks ensuring that the public benefits from the economic value of data. Government digitization creates efficiency gains but these have not translated into measurable public data value.

Indicator Scores:

1.1 Legislation on data ownership: Level 2 - Aware

1.2 Domestic data storage: Level 2 - Aware

1.3 Protection of cross-border data transfers: Level 1 - Initial

1.4 Inclusion of data value for the public: Level 2 - Aware

Dimension 2: Digital Infrastructure Independence (1.75/5.0)

Digital infrastructure independence displays islands of specific capability existing in a sea of foreign dependence, with a dimension average of 1.75. Independence of foundational hardware reaches Level 2 (Aware), with Egypt possessing the most mature fabless semiconductor design ecosystem in the MENA region, including Si-Ware Systems (MEMS and optical sensors), Mentor Graphics Cairo Design Center (Siemens subsidiary, ASIC/FPGA design), and Valeo Egypt (automotive semiconductors). Universities provide semiconductor design education, with the industry claiming capabilities reaching 5-7nm nodes. However, Egypt lacks any manufacturing capability, creating structural dependence—design capabilities cannot translate into production autonomy. The 2024 fab plan remains in the feasibility consultation stage, with no concrete investment commitments or timeline. Servers and network equipment are entirely procured from international suppliers.

Independence of foundational software reaches only Level 1 (Initial), the lowest indicator in this dimension, reflecting complete foreign dependence. The operating system market is dominated by Windows, iOS, and Android, with no identifiable indigenous OS development. Cloud platforms are entirely controlled by foreign providers such as AWS, Microsoft Azure, and Oracle, with the government actively deepening dependence through strategic partnerships (Microsoft Egypt Strategic MoU, AWS Egypt Data Center Plan) rather than developing indigenous alternatives. Database systems are primarily Oracle, Microsoft SQL Server, and MySQL, with no indigenous database platforms. Middleware systems rely on Oracle Fusion, SAP NetWeaver, and IBM products, with no indigenous middleware development.

Independence of application software reaches Level 2 (Aware), with outstanding performance in fintech and educational software sectors. Local companies such as Fawry (payment processing), Paymob (payment gateway), and Khazna (digital wallet) demonstrate application development capabilities. Educational software platforms including Nafham and Edraak serve the MENA market. However, enterprise and industrial software completely depends on foreign suppliers (SAP, Oracle, Microsoft Dynamics dominate ERP; AutoCAD and SOLIDWORKS dominate CAD). Critically, 92% of digital exports are services rather than products ($6.2 billion exports, only 8% software products), indicating that capabilities are deployed serving foreign companies rather than building domestic technological independence.

Independence of information security reaches Level 2 (Aware), demonstrating framework excellence but limited market and capabilities. Egypt achieved first-tier ranking in the 2024 ITU Global Cybersecurity Index (100/100 points, up from 23rd place in 2020), reflecting strong regulatory frameworks and institutional commitment. EG-CERT under the National Telecommunications Regulatory Authority (NTRA) operates the national CERT, providing incident response. The Cybercrime Law (2018) establishes the legal framework. However, the domestic cybersecurity market size is only $220-230 million, significantly below the Level 3 threshold of $500 million. Deployed security technologies primarily come from international suppliers (Cisco, Palo Alto Networks, Fortinet), with local companies mainly providing integration and consulting services.

Indicator Scores:

2.1 Independence of foundational hardware: Level 2 - Aware

2.2 Independence of foundational software: Level 1 - Initial

2.3 Independence of application software: Level 2 - Aware

2.4 Independence of information security: Level 2 - Aware

Dimension 3: Digital Governance Independence (2.25/5.0)

Digital governance independence displays complex engagement but systematic implementation gaps, with a dimension average of 2.25. Legislative capacity for digital affairs reaches Level 3 (Developing), with Egypt demonstrating rapid legislative enactment capability, with executive-led laws passed in 1-3 months (Personal Data Protection Law promulgated July 2020, Data Protection Law Amendment promulgated March 2023, National Data Protection Center Law promulgated June 2024). The comprehensive legal framework covers data protection, cybercrime, electronic transactions, and digital government. However, implementation delays are systematic—3.5 years elapsed between the Personal Data Protection Law's promulgation (July 2020) and implementing regulations (February 2024), with the Personal Data Protection Center remaining non-operational for four years. Executive dominance limits legislative independence, with limited parliamentary debate often occurring as formalistic approval after law promulgation.

Enforcement capacity for digital affairs reaches Level 2 (Aware), with extensive legal frameworks and enforcement activities but zero cases of platform behavior change. Cybercrime Law enforcement is active, handling thousands of cases from 2018-2024, but primarily targeting illegal content, fraud, and cyberbullying, rather than digital sovereignty-related violations. The E-Commerce Law is enforced by the Consumer Protection Agency, handling e-commerce disputes but with no documented enforcement against major platforms. Selective implementation favors security controls

over rights protection—website blocking is swiftly implemented (over 600 websites reportedly blocked), but the non-operation of the Personal Data Protection Center makes data rights unenforceable. There are no identifiable cases of foreign tech platforms changing behavior due to Egyptian enforcement.

Leadership in international digital technology rules reaches Level 2 (Aware), with active participation but limited concrete outcomes. Egypt has been an ITU Council member since 1973, hosts major conferences (2022 World Telecommunication Standardization Assembly), and participates in standards organizations (ISO, IEC, IEEE membership). However, it is not possible to enumerate 2-3 specific technical standards led by Egypt that have gained international adoption. Participation is primarily in implementing international standards rather than creating new ones, with a thin technical foundation limiting standards-setting contributions.

Leadership in international digital behavior rules reaches Level 2 (Aware), with formal leadership positions but no concrete rule-setting outcomes. Egypt holds positions including African Union ICT Commission Chair for North Africa, Arab AI Working Group leadership, and World Economic Forum Fourth Industrial Revolution Center regional hub. However, there are no identifiable Egyptian-initiated digital behavior rules adopted regionally or globally—African countries follow GDPR rather than Egyptian data protection frameworks, and Arab AI guidelines have not yet produced concrete binding rules. Participation shows activity but primarily as a participant rather than a rule-shaper.

Indicator Scores:

3.1 Legislative capacity for digital affairs: Level 3 - Developing

3.2 Enforcement capacity for digital affairs: Level 2 - Aware

3.3 Leadership in international digital technology rules: Level 2 - Aware

3.4 Leadership in international digital behavior rules: Level 2 - Aware

Dimension 4: Digital Capability Independence (2.25/5.0)

Digital capability independence reflects ambitious strategic visions undermined by structural constraints, with a dimension average of 2.25. Cutting-edge technology research and development reaches Level 2 (Aware), with annual patent output of 881-1,027, only 2-5% of the Level 3 threshold (10,000-50,000). R&D investment at 1.02% of GDP (2020), below the Level 3 threshold of 1.5%, with the private sector accounting for only 2.7%, indicating R&D is primarily a public sector activity. Research institutions include the Electronics Research Institute, Central Electronics Engineering Research Institute, and universities, but absolute output is minimal. Artificial intelligence and machine learning research is growing, but primarily in applications rather than fundamental research.

Talent cultivation in universities reaches Level 2 (Aware), with massive output accompanied by catastrophic attrition. Egypt annually produces approximately 207,000 STEM graduates (approximately 120,000 engineering, 55,000 computer science, 32,000 other technical fields), exceeding the Level 3 threshold (50,000), but quality and retention issues severely constrain actual capability contributions. The 86.5% STEM graduate emigration rate is a devastating constraint—Egypt becomes a STEM training provider for destination countries, with approximately 180,000 STEM graduates leaving annually and only 28,000 remaining in the domestic labor force. Universities including Cairo University and Ain Shams University provide STEM education, but educational quality is uneven, with high unemployment rates.

Industry engineering capabilities reach Level 2 (Aware), with 240,000 IT professionals creating $6.2 billion in exports, but 92% being services indicates a structural bias toward outsourcing rather than product development. The IT sector employs approximately 240,000 workers, mainly in software services, systems integration, and BPO. Sectors such as fintech (Fawry, Paymob) and fabless semiconductor design demonstrate specialized strengths, but at small absolute scale. Enterprise software development capabilities are primarily customization and integration of foreign platforms rather than creation of indigenous products. The export structure (92% services versus 8% products)

indicates that capabilities are deployed serving foreign companies rather than building domestic technological independence, deepening rather than reducing dependence.

Coordination of digital technology with national development strategies reaches Level 3 (Developing), with 8-9 years of sustained implementation producing concrete outcomes. Vision 2030 (2016), Digital Egypt Initiative, and National AI Strategy 2019 provide a comprehensive framework with clear integration of digital development with national priorities. Concrete outcomes include government data center migration (114 entities), 4G/5G deployment (4G covering 99% of the population, 5G pilots starting in 2021), digital government services (150+ e-services), and e-payment growth. The Ministerial Committee for Digitization coordinates cross-departmental efforts, with EGP 15 billion allocated to digital infrastructure. However, major implementation gaps persist—the Personal Data Protection Center remains non-operational, fab plans remain unfunded, and digital export targets ($10 billion by 2025) remain unachieved.

Indicator Scores:

4.1 Cutting-edge technology research and development: Level 2 - Aware

4.2 Talent cultivation in universities: Level 2 - Aware

4.3 Industry engineering capabilities: Level 2 - Aware

4.4 Coordination of digital technology with national development strategies: Level 3 - Developing

Summary

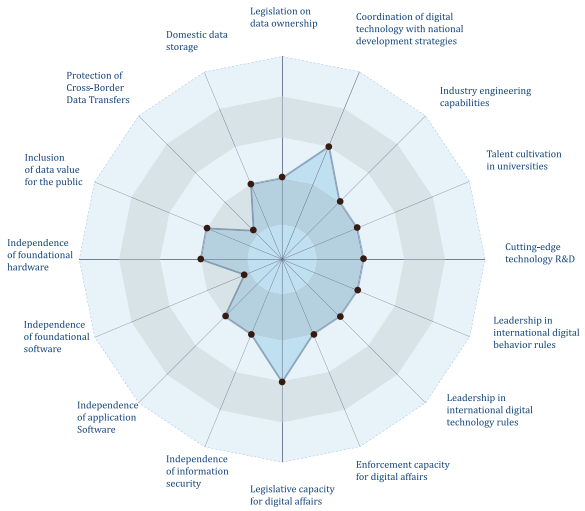
Egypt's DSI score of 1.94 presents a pattern of "framework sovereignty rather than operational sovereignty"—the ability to formulate comprehensive digital governance frameworks demonstrates awareness, but failure to achieve the institutional independence, technical capabilities, and enforcement effectiveness required for genuine digital autonomy. The country demonstrates the ability across all four dimensions to formulate sound frameworks, participate in international affairs, and build specific capabilities, but systematic implementation gaps prevent progression from awareness toward development and competitiveness.

The most notable characteristic is the persistent gap between legislation and implementation. Rapid legislative enactment (laws passed in 1-3 months) contrasts with delayed implementation (Personal Data Protection Center non-operational for four years, implementing regulations delayed by 3.5 years). This pattern is not accidental but systematic—measures enhancing state control are rapidly implemented (website blocking, surveillance systems), while measures constraining state power or foreign platforms are indefinitely delayed (data protection rights, platform regulation). Selective implementation favors security controls over rights protection, demonstrating how political-economic constraints shape sovereignty trajectories.

Structural constraints profoundly limit capability building. The 86.5% STEM graduate emigration rate is catastrophic attrition—annual production of 207,000 STEM graduates but only 28,000 remaining domestically makes Egypt a training provider for destination countries rather than a builder of domestic capacity. The IT sector is structurally biased toward service outsourcing (92% of exports are services), with capabilities deployed serving foreign companies rather than building domestic technological independence. Complete dependence on foundational software (Windows, AWS, Oracle, SAP), with government strategic partnerships further deepening dependencies rather than developing alternatives. Annual patent output of 881-1,027 is only 2-5% of the Level 3 threshold, R&D investment at 1.02% of GDP is below the 1.5% threshold, with the private sector accounting for only 2.7%.

Egypt's transition from framework sovereignty to operational sovereignty requires: (1) operationalizing the Personal Data Protection Center within a clear timeline to make legal rights enforceable; (2) urgently addressing talent drain through incentives to retain STEM graduates; (3) strategic transition from services to products, developing indigenous technology products rather than merely serving foreign companies; (4) addressing the selective implementation pattern to balance state control with rights protection. The

current trajectory suggests that without addressing political-economic constraints and resource limitations, Egypt will continue to display sound frameworks while lacking operational implementation, maintaining positioning between Levels 1-2, demonstrating awareness but failing to translate into genuine capability and independence.



Egypt Digital Sovereignty Index Assessment Results

Dimension Average Scores:

- Dimension 1 - Data Ownership Independence: 1.75/5.0
- Dimension 2 - Digital Infrastructure Independence: 1.75/5.0
- Dimension 3 - Digital Governance Independence: 2.25/5.0
- Dimension 4 - Digital Capability Independence: 2.25/5.0

Ethiopia Digital Sovereignty Index Assessment

Assessment Date: October 16, 2025 **Total DSI Score**: 1.81/5.0 **Country Code**: ET

Overview

Ethiopia scores 1.81 out of 5 in the Digital Sovereignty Index assessment, presenting an emerging digital sovereignty posture characterized by recently established comprehensive legislative frameworks with limited operational implementation and significant infrastructure dependencies. The country is in transition between Initial (Level 1) and Aware (Level 2) stages, with strategic coordination reaching Level 3 (Developing) and data ownership legislation at Level 3. The Personal Data Protection Proclamation 1321/2024, promulgated in July 2024, represents a sophisticated legal framework aligned with GDPR principles, featuring potentially severe penalties (up to 4% of global turnover plus 10 years imprisonment), but is completely untested with zero enforcement track record.

Despite foundational weaknesses, Ethiopia demonstrates emerging capabilities at the application software level (domestic companies like ZalaTech, PRIME, Simbo, with a $523 million market growing at 11-13% annually) and talent cultivation (30% growth in STEM enrollment, 5 million programmers initiative, projected 400,000 tech jobs by 2025). The "Digital Ethiopia 2025" strategy shows strong coordination of digital transformation with broader economic development objectives, with concrete e-government progress (over 130 digitized services, 40 million internet users, measurable economic impact of 5.3% of GDP).

However, structural constraints profoundly limit the sovereignty trajectory. Complete dependency on foreign foundational technologies—no domestic chips, operating systems, or databases, with even operational domestic infrastructure (Ethio Telecom cloud services with 90+ customers) entirely reliant on foreign technology stacks (Huawei). Data localization requirements operate atop foreign infrastructure, creating sovereignty vulnerabilities. The legislative framework is only 3 months old with no enforcement precedents, making it untested policy rather than proven capability. Global innovation ranking of 130th, universities focused on adoption rather than innovation, no internationally recognized ICT patents or breakthroughs. Not a WTO member, no leadership positions in technical standards bodies, a rule-taker rather than rule-maker in digital governance forums.

Dimension 1: Data Ownership Independence (2.25/5.0)

Ethiopia's data governance reveals a paradox of sophisticated legal frameworks with complete absence of operational implementation, scoring 2.25 for this dimension, positioned between Aware and Developing. Legislation on data ownership reaches Level 3 (Developing), with the Personal Data Protection Proclamation 1321/2024 of July 2024 establishing a comprehensive framework comparable to GDPR levels, covering data subject rights (access, rectification, erasure, restriction of processing, portability), data controller obligations, and cross-border transfer rules. The law mandates establishment of the Personal Data Protection Authority as an independent regulatory body with powers of inspection, investigation, and penalties up to 4% of global turnover plus 10 years imprisonment. Article 26 of the Constitution provides the foundation for privacy rights.

However, a critical weakness is temporality—these frameworks are only 3 months old with no enforcement precedents. The Personal Data Protection Authority has not yet been established, there is no operational enforcement capacity, and no published implementation guidelines or regulations. The legal text is sophisticated but unverified by practical application. Zero documented cases of data protection violation enforcement, zero cases of foreign platforms changing behavior due to Ethiopian data protection provisions.

Domestic data storage reaches Level 2 (Aware), with Article 11 of the Personal Data Protection Proclamation requiring data controllers processing Ethiopian personal data to store data within Ethiopia's borders, unless data subjects explicitly consent to cross-border transfers or the destination country provides adequate protection. However, the absence of operational agencies monitoring compliance, lack of published lists of countries approved for cross-border transfers, and lack of standard contractual clauses means localization requirements are legally mandated but practically unenforced. Critically, even if implemented, localization operates atop foreign technology stacks (Huawei cloud), limiting genuine sovereignty.

Protection of cross-border data transfers reaches Level 2 (Aware), with Articles 11-12 of the Personal Data Protection Proclamation establishing detailed cross-border transfer rules requiring adequacy decisions or standard contractual clauses. However, like localization, these provisions are completely unimplemented. Zero adequacy decisions issued, no approved standard contractual clauses, no operational permit systems. Inclusion of data value for the public reaches Level 2 (Aware), with Digital Ethiopia 2025 identifying data as a strategic resource and government digitization creating efficiency gains, but lacking systematic data value capture mechanisms, data dividend schemes, or regulatory frameworks ensuring the public benefits from data economic value.

Indicator Ratings:

1.1 Legislation on data ownership: Level 3 - Developing

1.2 Domestic data storage: Level 2 - Aware

1.3 Protection of cross-border data transfers: Level 2 - Aware

1.4 Inclusion of data value for the public: Level 2 - Aware

Dimension 2: Digital Infrastructure Independence (1.50/5.0)

Digital infrastructure independence is the weakest dimension, scoring 1.50, firmly in the Initial stage with emerging Aware elements, revealing near-complete dependency on foreign foundational technologies. Both independence of foundational hardware and foundational software reach only Level 1 (Initial). Ethiopia has no domestic semiconductor production, no chip design capabilities, and complete reliance on imported chips (primarily from China, Taiwan, Korea via Chinese supply chains). No server or network equipment manufacturing, with all hardware procured from international suppliers (Huawei dominates telecommunications infrastructure, with ZTE and Ericsson also present).

Independence of foundational software shows complete dependence on foreign platforms. The operating system market is dominated by Windows, iOS, and An-

droid, with no identifiable domestic operating system development. For cloud platforms, Ethio Telecom provides cloud services (90+ customers, mainly government agencies), but this is entirely based on Huawei technology stacks, representing local deployment of foreign technology rather than indigenous platforms. Database systems are primarily Oracle, MySQL, and Microsoft SQL Server, with no indigenous database platforms. Middleware systems rely on international products with no domestic middleware development.

Independence of application software reaches Level 2 (Aware), demonstrating emerging capabilities. Domestic companies like ZalaTech (mobile banking and payments), PRIME (education software), and Simbo (digital wallets) showcase application development capabilities. The application software market is valued at $523 million with annual growth of 11-13%. Government e-government platforms represent indigenous application capabilities (over 130 digitized services). However, enterprise and productivity software is completely dominated by foreign platforms (Microsoft Office, SAP, Oracle), with local applications primarily running atop Android and iOS, representing integration into foreign ecosystems.

Independence of information security reaches Level 2 (Aware), displaying operational capabilities but limited scale. The Information Network Security Agency (INSA) provides national cybersecurity coordination, claiming 97% attack defense rates and handling thousands of annual incidents. The Computer Crime Proclamation (2016) establishes a legal framework. However, the domestic cybersecurity market is minuscule with no identifiable indigenous cybersecurity product companies. Deployed security technologies primarily come from international suppliers (Huawei, Cisco, Fortinet), with local capabilities concentrated on government surveillance rather than commercial cybersecurity products.

Indicator Ratings:

2.1 Independence of foundational hardware: Level 1 - Initial

2.2 Independence of foundational software: Level 1 - Initial

2.3 Independence of application software: Level 2 - Aware

2.4 Independence of information security: Level 2 - Aware

Dimension 3: Digital Governance Independence (1.50/5.0)

Digital governance independence scores 1.50, in the Initial/Aware stage, with significant divergence between legislative capacity (Aware) and international influence (Initial). Legislative capacity for digital affairs reaches Level 2 (Aware), with Ethiopia having formulated multiple digital laws in recent years—Personal Data Protection Proclamation (2024), National Artificial Intelligence Policy (2024), Computer Crime Proclamation (2016), Telecommunications Proclamation (2019 revision)—demonstrating the ability to adapt international frameworks to local contexts. However, the legislative process is primarily administratively driven rather than parliamentary debate, with limited public participation and systematic implementation delays.

Enforcement capacity for digital affairs reaches Level 2 (Aware), with legal mandates existing but unverified. Computer Crime Proclamation enforcement primarily targets illegal content and national security threats rather than digital sovereignty-related violations. No documented data protection or platform regulation enforcement actions against digital platforms. INSA enforces cybersecurity laws but primarily focuses on government systems rather than private sector compliance. No identifiable cases of foreign tech platforms changing behavior due to Ethiopian enforcement.

Leadership in international digital technology rules reaches only Level 1 (Initial), with minimal international influence. Ethiopia is not a WTO member, limiting participation in trade-related digital rules. No leadership positions in technical standards bodies (ISO, ITU, IEEE), with no identifiable Ethiopian-led technical standards gaining international adoption. Participation is primarily in implementing international standards rather than creating new standards.

Leadership in international digital behavior rules likewise reaches only Level 1 (Initial), with Ethiopia

being a rule-taker rather than rule-maker in digital governance forums. Participation in African Union digital initiatives and United Nations forums exists, but without leadership positions or concrete rule-making contributions. No identifiable Ethiopian-initiated digital behavior rules gaining regional or global adoption. Digital governance positions typically align with African consensus rather than independent alternatives.

Indicator Ratings:

3.1 Legislative capacity for digital affairs: Level 2 - Aware

3.2 Enforcement capacity for digital affairs: Level 2 - Aware

3.3 Leadership in international digital technology rules: Level 1 - Initial

3.4 Leadership in international digital behavior rules: Level 1 - Initial

Dimension 4: Digital Capability Independence (2.00/5.0)

Digital capability independence scores 2.00, in the Aware stage, with significant strength in strategic coordination (Level 3) but weakness in R&D (Level 1), revealing Ethiopia's focus on building human capital and strategic alignment rather than cutting-edge technological innovation. Cutting-edge technology research and development reaches only Level 1 (Initial), with Ethiopia ranking 130th in the Global Innovation Index, R&D spending at 0.6% of GDP (far below the 1.5% threshold for Level 3), and no internationally recognized ICT patents or technological breakthroughs. Universities focus on technology adoption and implementation rather than fundamental research, with research primarily at the application level.

Talent cultivation in universities reaches Level 2 (Aware), demonstrating positive trends. STEM enrollment grew 30% (2020-2023), universities provide computer science and engineering education, and the government launched a 5 million programmers initiative with projected 400,000 tech jobs by 2025. However, absolute graduate numbers remain relatively limited, education quality is uneven, and talent outflow persists (many graduates seek overseas opportunities). Engineering education mainly concentrates on using foreign technologies rather than developing indigenous technologies.

Industry engineering capabilities reach Level 2 (Aware), emerging but small-scale. Domestic software companies like ZalaTech, PRIME, and Simbo demonstrate application development capabilities, but primarily in mobile applications and digital services rather than platform or infrastructure development. The IT sector employs approximately 200,000-300,000 workers, mainly in services, systems integration, and BPO. Application software market growth of 11-13% annually shows vitality, but absolute scale ($523 million) remains small. Enterprise software development capabilities are primarily customization and integration of foreign platforms.

Coordination of digital technology with national development strategies reaches Level 3 (Developing), the strongest indicator in this dimension. The "Digital Ethiopia 2025" strategy (2020-2025) demonstrates sophisticated strategic thinking with clear integration across multiple national development frameworks (Ten Year Development Plan, National Transformation Agenda). Concrete outcomes include government digitization (over 130 e-services), mobile network expansion (40 million internet users), digital payment growth, and e-government progress. The digital economy contributes 5.3% of GDP, demonstrating measurable economic impact. However, strategic ambition exceeds infrastructure and enforcement implementation capacity, creating implementation gaps that may undermine strategic objectives.

Indicator Ratings:

4.1 Cutting-edge technology research and development: Level 1 - Initial

4.2 Talent cultivation in universities: Level 2 - Aware

4.3 Industry engineering capabilities: Level 2 - Aware

4.4 Coordination of digital technology with national development strategies: Level 3 - Developing

Summary

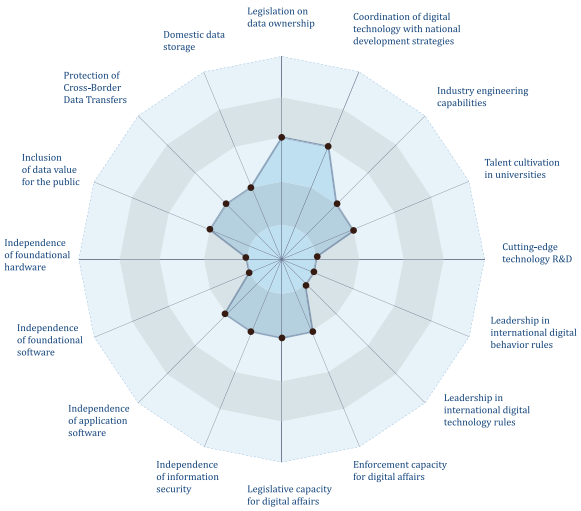
Ethiopia's DSI score of 1.81 reflects a nation in the early stages of digital sovereignty development, with significant recent policy acceleration but facing substantial implementation challenges. The assessment reveals three defining characteristics: legislative modernity coexisting with enforcement immaturity, infrastructure dependency constraining sovereignty, and strategic vision exceeding current capabilities.

The gap between legislation and implementation is a core feature. Ethiopia has promulgated contemporary digital frameworks—PDPP 2024 (aligned with GDPR), National AI Policy 2024, Computer Crime Proclamation 2016—demonstrating legislative capacity to address cutting-edge digital governance challenges. However, these frameworks remain untested, with PDPP only 3 months old and zero enforcement actions despite strong penalty provisions (4% of global turnover plus 10 years imprisonment). The Personal Data Protection Authority has not yet been established, there is no operational enforcement capacity, and no published implementation guidelines. Zero cases of foreign platforms changing behavior due to Ethiopian enforcement.

Infrastructure dependency creates structural limitations. Complete dependence on foreign foundational technologies—no domestic chips, operating systems, or databases—poses fundamental constraints on digital sovereignty aspirations. Data localization requirements operate atop foreign infrastructure (Huawei cloud stacks), creating sovereignty vulnerabilities. Even when laws require data storage domestically, the technological platforms managing that data remain owned and controlled by foreign companies. This dependency limits genuine sovereignty because infrastructure providers may retain access and control capabilities over data regardless of physical storage location.

Strategic coordination (Level 3) demonstrates sophisticated strategic thinking in Digital Ethiopia 2025, with clear integration across multiple national development frameworks producing concrete outcomes (over 130 e-services, 40 million internet users, 5.3% digital economy contribution to GDP). However, strategic ambition exceeds infrastructure and enforcement implementation capacity, creating implementation gaps. The 30% growth in STEM enrollment and 5 million programmers initiative demonstrate commitment to talent cultivation, but Global Innovation ranking of 130th, R&D spending at 0.6% of GDP, and no internationally recognized ICT patents indicate weak innovation capabilities.

The critical phase is implementation. Ethiopia's digital sovereignty will not be determined by the sophistication of laws promulgated in 2024, but by the enforcement actions taken in 2025-2026, the infrastructure investments made to support data localization, and the capabilities built to implement strategic visions. Without translating legal frameworks into practical capabilities, Ethiopia risks permanently remaining in the "Aware" digital sovereignty stage, unable to achieve meaningful independence. What is needed: (1) operationalize the Personal Data Protection Authority and begin enforcement; (2) invest in indigenous infrastructure capabilities to reduce foreign technology dependency; (3) shift from strategic planning to operational implementation; (4) build R&D capabilities moving from adoption to innovation.



Ethiopia Digital Sovereignty Index Assessment Results

Dimension Average Scores:

- Dimension 1 - Data Ownership Independence: 2.25/5.0
- Dimension 2 - Digital Infrastructure Independence: 1.50/5.0
- Dimension 3 - Digital Governance Independence: 1.50/5.0
- Dimension 4 - Digital Capability Independence: 2.00/5.0

Iran Digital Sovereignty Index Assessment

Assessment Date: October 16, 2025 **Total DSI Score**: 1.94/5.0 **Country Code**: IRN

Overview

Iran's digital sovereignty development exhibits extreme contradictions: on one hand, it demonstrates clear policy awareness and strategic planning, possessing a complete governance architecture including the National Information Network (NIN) and the Supreme Council of Cyberspace; on the other hand, it is trapped in profound technological isolation and capability stagnation. Among the 16 assessment indicators, only 2 indicators reach Level 3 (Developing), 11 indicators remain at Level 2 (Aware), and another 3 indicators are at Level 1 (Initial) status. This "aware but constrained" state stems from comprehensive international sanctions and geopolitical isolation, which prevent Iran from accessing advanced technologies, participating in international standard-setting, and engaging in technological cooperation. The data that best reflects Iran's predicament includes: near-zero participation in international digital governance, with Dimension 3 (Digital Governance Independence) scoring only 1.50/5.0, making it one of the worst-performing countries in this dimension among all assessed countries; severe brain drain causes excellent engineers and researchers to emigrate overseas seeking development opportunities, weakening the accumulation of domestic technical capabilities.

A deeper challenge lies in the fundamental misalignment between Iran's digital capacity building and digital sovereignty principles. Data localization (Level 3) and cybersecurity capabilities (Level 3) are the only two indicators reaching "Developing" level, but these capabilities primarily serve state surveillance and content control rather than protecting citizens' data rights or promoting economic development. Enforcement mechanisms target content censorship rather than foreign platform regulation, and the legislative framework prioritizes national security over privacy protection. This directional bias means that even when demonstrating certain technical capabilities, they cannot be translated into the comprehensive digital sovereignty encompassing economic, social, and strategic dimensions as anticipated by the framework. The technological ceiling created by sanctions traps Iran in a self-reinforcing cycle of exclusion: inability to access advanced equipment and specialized software → limited R&D capabilities → stagnant industrial production → intensified brain drain → further weakening of capabilities. Without fundamental adjustments to the geopolitical landscape, Iran's digital sovereignty development appears structurally difficult to break through.

Dimension 1: Data Ownership Independence (2.00/5.0)

Iran demonstrates clear policy awareness in the data ownership dimension, advancing data localization through the National Information Network initiative, but the overall framework suffers from severe implementation lag and directional bias. Data localization is the relatively well-developed area in this dimension (Level 3), with the government requiring that government data must be stored domestically and reinforcing localization measures through systematic blocking of foreign platforms such as Facebook, Twitter, and YouTube. Domestic cloud infrastructure includes approximately 250 cloud service providers such as Arvan Cloud and HPDS, forming a certain market scale. However, this data localization serves more for surveillance and content control objectives rather than economic sovereignty or citizen rights protection, representing a fundamental misalignment with the core principles of digital sovereignty.

Legislative deficiencies further expose the transformation dilemma from awareness to implementation. Although Iran has enacted basic legislation such as the Computer Crimes Law (2009) and E-Commerce Law, a comprehensive Data Protection Bill has been under review since 2019 without passage, showing the legislative process is blocked. Existing legislation prioritizes national security and control objectives rather than personal data rights protection. Protection of cross-border data transfers (Level 2) remains at the level of policy discourse, lacking a comprehensive framework for systematically identifying, organizing, and monetizing public data assets. The weakest link is inclusion of data value for the public (Level 1), where citizens are almost not regarded as stakeholders entitled to share data value, lacking enforceable data rights, data portability mechanisms, or frameworks for deriving value from personal data. International sanctions further limit Iran's ability to participate in the global data economy, making the space for data value creation and sharing extremely narrow.

Indicator Scores:

1.1 Legislation on data ownership: Level 2 - Aware

1.2 Domestic data storage: Level 3 - Developing

1.3 Protection of cross-border data transfers: Level 2 - Aware

1.4 Inclusion of data value for the public: Level 1 - Initial

Dimension 2: Digital Infrastructure Independence (2.25/5.0)

Iran faces severe sanctions constraints in the digital infrastructure dimension. Although it has developed certain domestic infrastructure through the National Information Network initiative, deep dependence on foreign technologies persists, forming a fragile pattern of "local control, external dependence." In terms of foundational hardware (Level 2), Iran has established government-controlled backbone networks and domestic data centers, possessing considerable control over critical network infrastructure components. However, sanctions fundamentally limit the independence of network infrastructure, with core network components, telecommunications equipment, and advanced infrastructure elements continuing to come from foreign suppliers, facing major obstacles in accessing advanced network equipment. At the foundational software level (Level 2), the situation is similar. Although it has approximately 250 domestic cloud service providers such as Arvan Cloud, it lacks advanced chip manufacturing capabilities—the cornerstone of computing infrastructure independence. Although Iran has developed 32-bit processor designs, there is no evidence of advanced semiconductor manufacturing facilities capable of producing competitive chips at modern process nodes.

Independence of application software (Level 2) reflects a huge gap between policy will and market reality. The National Software Movement aims to encourage local software production and reduce dependence on foreign platforms, but foreign software dominates Iran's software infrastructure: Microsoft Windows holds an overwhelming market share in operating systems, and Microsoft Office products dominate the productivity software sector. The only area reaching "Developing" level is independence of information security (Level 3), where Iran has developed substantial cybersecurity capabilities, including offensive and defensive operations. Multiple Advanced Persistent Threat (APT) groups

associated with Iranian national entities (including APT33, APT34, APT35, etc.) demonstrate technical capabilities in malware development, network intrusion, data exfiltration, and infrastructure manipulation. However, these capabilities are primarily offensive rather than defensive, and sanctions limit access to advanced defensive cybersecurity technologies, making Iran's cybersecurity capabilities more a reflection of asymmetric tactics rather than a comprehensive information security system.

Indicator Scores:

2.1 Independence of foundational hardware: Level 2 - Aware

2.2 Independence of foundational software: Level 2 - Aware

2.3 Independence of application software: Level 2 - Aware

2.4 Independence of information security: Level 3 - Developing

Dimension 3: Digital Governance Independence (1.50/5.0)

Digital governance is Iran's biggest shortcoming in digital sovereignty development, with a dimension score of 1.50/5.0 ranking at the bottom among all assessed countries. The core problem lies in the almost complete absence of international participation and fundamental misalignment of governance orientation. At the domestic governance level, Iran maintains an active legislative process through the Supreme Council of Cyberspace (Level 2), with the Computer Crimes Law (2009) and subsequent cyber-related legislation demonstrating institutional capacity. Enforcement capacity (Level 2) is manifested through the Cyber Police (FATA) and judicial institutions, possessing the ability to implement internet restrictions, block foreign platforms, and enforce compliance with domestic regulations. However, the orientation of these capabilities fundamentally misaligns with digital sovereignty goals: legislation emphasizes surveillance, censorship, and content control rather than protecting digital economic interests, data sovereignty, or citizen rights; enforcement work overwhelmingly focuses on censorship and surveillance rather than regulating commercial behavior of foreign platforms or enforcing penalties for data sovereignty violations.

The absence at the international participation level constitutes the most severe structural obstacle. Leadership in international digital technology rules (Level 1) and leadership in international digital behavior rules (Level 1) are both in initial states. Comprehensive international sanctions and geopolitical isolation effectively exclude Iran from key technology standards development organizations (ITU, ISO, IEC, IEEE, etc.), Internet Governance Forums, and multilateral digital policy initiatives. Without participation in international organizations, Iran cannot leverage multilateral frameworks to enhance digital sovereignty, nor can it participate in formulating global digital governance rules. This isolation not only limits Iran's voice but also blocks possibilities for knowledge transfer and capacity building through international cooperation, placing Iran in a completely marginalized position in the global digital governance system. Sanctions-driven isolation traps Iran in a vicious cycle: inability to participate in international standard-setting → technological pathways diverge from international mainstream → further exclusion from international cooperation → capability gap continues to widen.

Indicator Scores:

3.1 Legislative capacity for digital affairs: Level 2 - Aware

3.2 Enforcement capacity for digital affairs: Level 2 - Aware

3.3 Leadership in international digital technology rules: Level 1 - Initial

3.4 Leadership in international digital behavior rules: Level 1 - Initial

Dimension 4: Digital Capability Independence (2.00/5.0)

Iran demonstrates certain foundational capabilities in the digital capability dimension but faces severe brain drain and technology access barriers, trapping capacity building in a vicious cycle of "cultivation-drain-weakening." Cutting-edge technology research and development (Level 2) is maintained through the university system and government-supported research institutions, with universities conducting research in computer science, electrical engineering, and related fields, and some semiconductor design work taking place in academic institutions. However, sanctions fundamentally limit R&D capabilities: facing major obstacles in accessing advanced research equipment, specialized software tools, and international collaboration opportunities. The talent cultivation (Level 2) system is relatively complete, with multiple universities offering degree programs in digital technology fields, and the government's knowledge-based economy framework emphasizing STEM education as a policy priority. However, severe brain drain undermines the effectiveness of talent supply, with many of the best graduates emigrating to Western countries. Although Iran cultivates technical workers, the country does not fully reap the economic and strategic returns from its educational investments.

Industry engineering capabilities (Level 2) are primarily manifested in the cybersecurity field, where the sophistication of Iranian cyber operations (requiring expertise in malware development, network protocols, and system vulnerabilities) indicates substantial engineering capabilities. However, engineering capabilities face constraints similar to those in R&D, with limited access to advanced design tools restricting the development of engineering capabilities in semiconductors and hardware. At the level of coordination with national development strategies (Level 2), the government's knowledge-based economy strategy and Tech Vision 2025 document incorporate data economy elements, indicating awareness of data economy potential, but transformation from awareness to implementation remains limited. Sanctions further limit Iran's ability to participate in the global data economy, restricting opportunities for data-related exports, digital service provision, and integration into international data value chains. All indicators in this dimension remain at Level 2 "Aware," reflecting the structural dilemma of Iran's digital capability development: possessing basic educational systems and R&D frameworks but unable to translate them into substantive technological breakthroughs and industrial capabilities.

Indicator Scores:

4.1 Cutting-edge technology research and development: Level 2 - Aware

4.2 Talent cultivation in universities: Level 2 - Aware

4.3 Industry engineering capabilities: Level 2 - Aware

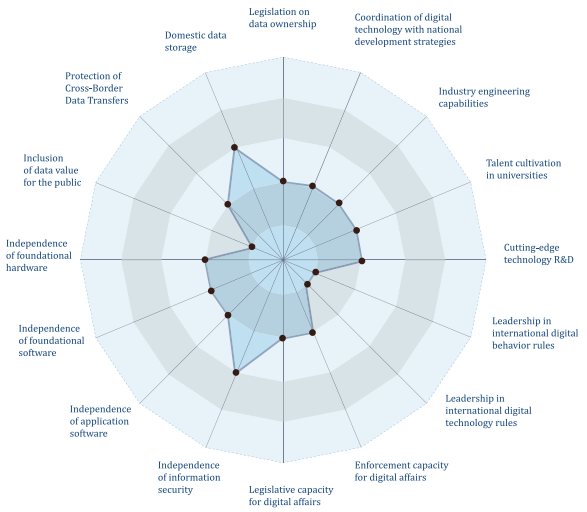
4.4 Coordination of digital technology with national development strategies: Level 2 - Aware

Summary

Iran's digital sovereignty situation presents a unique pattern of "aware but constrained," with a total DSI score of 1.94/5.0 at the lowest level among all assessed countries, and none of the 16 indicators reaching Level 4 or above. The root of this state lies in technological isolation caused by comprehensive international sanctions, constituting the most severe structural constraint and creating a self-reinforcing cycle of exclusion and underdevelopment. Sanctions prevent access to advanced technologies, manufacturing equipment, specialized software, and international cooperation, directly constraining infrastructure independence, R&D capabilities, and industrial production; geopolitical isolation excludes Iran from international standards bodies, multilateral digital governance initiatives, and technology partnerships, blocking possibilities for knowledge transfer and capacity building. The most telling reflection of this predicament is the 1.50 score in Dimension 3 (Digital Governance Independence) and Level 1 ratings for both international participation indicators, showing Iran's completely marginalized position in the global digital governance system.

A deeper challenge lies in the misalignment between capacity building orientation and digital sovereignty principles, making it difficult for Iran to translate even the few areas reaching "Developing" level into com-

prehensive digital sovereignty. Data localization and cybersecurity capabilities primarily serve surveillance and control objectives, enforcement targets content censorship rather than platform regulation, and legislation prioritizes national security over citizen rights. This directional bias means that improvements in technical capabilities have not brought comprehensive digital sovereignty development in economic, social, and strategic dimensions. Without sanctions relief or breakthrough innovations to circumvent technology access barriers, Iran's progress from Level 2 to higher levels remains structurally blocked in most dimensions. Iran's digital sovereignty trajectory is determined more by geopolitical dynamics than domestic policy choices, creating a unique state of "constrained awareness" in the global digital sovereignty landscape.



Iran Digital Sovereignty Index Assessment Results

Dimension Average Scores:

- Dimension 1 (Data Ownership Independence): 2.00/5.0
- Dimension 2 (Digital Infrastructure Independence): 2.25/5.0
- Dimension 3 (Digital Governance Independence): 1.50/5.0
- Dimension 4 (Digital Capability Independence): 2.00/5.0

Saudi Arabia Digital Sovereignty Index Assessment

Assessment Date: October 15, 2025 **Total DSI Score**: 2.5/5.0 **Country Code**: SA

Overview

Saudi Arabia scores 2.5 out of 5 in the Digital Sovereignty Index assessment, presenting a distinctive digital sovereignty profile: comprehensive regulatory frameworks and exceptional strategic coordination capacity, but constrained by limited enforcement track record and severe infrastructure dependencies. The country achieves Level 3 (Developing) across all Data Ownership Independence indicators, reflecting the GDPR-aligned Personal Data Protection Law (2021), explicit data localization requirements, and stringent cross-border data transfer controls. Strategic coordination capacity reaches Level 4 (Competent) through Vision 2030's integration of digital technology into 67% of national development objectives, a proportion that is globally leading.

However, enforcement implementation only began in September 2024, with no enforcement cases recorded to date. Infrastructure independence is severely limited (Dimension 2: 2.0/5.0), with complete dependence on foreign foundational software and no semiconductor manufacturing capabilities. International influence (Dimension 3 indicators 3.3-3.4) remains at awareness-level participation, without standard-setting or rule-shaping capabilities. Saudi Arabia's greatest strength lies in its comprehensive policy architecture and systematic strategic planning, but the critical weakness is the lag in implementation and technological capability dimensions.

Dimension 1: Data Ownership Independence (3.0/5.0)

Saudi Arabia demonstrates robust performance in Data Ownership Independence, with all four indicators achieving Level 3 (Developing). The Personal Data Protection Law (PDPL) enacted in 2021 establishes a comprehensive data protection framework comparable to GDPR, covering data subject rights, enforcement agency authority, and compliance requirements. The Saudi Data and Artificial Intelligence Authority (SDAIA), as the primary enforcement agency, possesses powers to suspend data processing, maintain a national registry of data processors, and impose administrative penalties.

Data localization requirements explicitly mandate that personal data processing must be conducted domestically. Major foreign cloud service providers including Amazon AWS, Microsoft Azure, and Oracle Cloud have established data center facilities in Riyadh and Jeddah to comply with localization requirements. Cross-border data transfer regulations exceed GDPR standards in certain aspects, requiring explicit consent from data subjects, adequacy assessments of destination jurisdictions, and the use of standard contractual clauses as safeguard mechanisms.

The critical challenge, however, is that full PDPL enforcement only commenced in September 2024, and to date there are no recorded enforcement cases, making it impossible to assess deterrent effectiveness and behavioral compliance patterns. The maximum penalty ceiling (5 million Saudi Riyals / approximately $1.3 million USD) is substantially lower than GDPR thresholds (20 million euros or 4% of global revenue), potentially limiting deterrent effect on large multinational technology companies.

Indicator Scores:

1.1 Legislation on data ownership: Level 3 - Developing

1.2 Domestic data storage: Level 3 - Developing

1.3 Protection of cross-border data transfers: Level 3 - Developing

1.4 Inclusion of data value for the public: Level 3 - Developing

Dimension 2: Digital Infrastructure Independence (2.0/5.0)

Digital Infrastructure Independence is Saudi Arabia's weakest dimension, with an average score of only 2.0. Independence of foundational software receives a Level 1 rating (Initial), the only Level 1 indicator in the entire assessment, reflecting the country's complete dependence on foreign technology for operating systems, databases, middleware, and cloud platforms. Microsoft Windows dominates desktop operating systems with 86% market share, mobile computing relies entirely on Android and iOS, and there is no evidence of any domestic operating system development work.

In foundational hardware, Saudi Arabia currently has no domestic semiconductor manufacturing capabilities and is completely dependent on imported chips. Although Vision 2030 lists semiconductor industry development as a strategic priority and has announced major projects such as Foxconn's $9 billion chip manufacturing facility investment, these investments have not yet translated into operational capabilities. In application software, there are approximately 35 domestic ERP solutions and industry-specific application providers, but international vendors SAP, Oracle, and Microsoft still dominate the enterprise application market, with most domestic companies primarily serving as system integrators rather than original software developers.

Information security is relatively stronger (Level 3), with the National Cybersecurity Authority (NCA) establishing a comprehensive regulatory framework and Essential Cybersecurity Controls (ECC) through the Cybersecurity Law. However, domestic cybersecurity capabilities are mainly concentrated in consulting services rather than product development, with organizations typically deploying security technologies from American and Israeli manufacturers.

Indicator Scores:

2.1 Independence of foundational hardware: Level 2 - Aware

2.2 Independence of foundational software: Level 1 - Initial

2.3 Independence of application software: Level 2 - Aware

2.4 Independence of information security: Level 3 - Developing

Dimension 3: Digital Governance Independence (2.25/5.0)

The Digital Governance Independence dimension presents a significant asymmetry between legislative and enforcement capacities. Legislative capacity reaches Level 3 (Developing), with significantly accelerated legislative activity during 2020-2024, establishing a comprehensive framework covering data protection, cybersecurity, AI ethics, and platform governance. Laws and regulations including the Personal Data Protection Law (2021), the Cybersecurity Law (Royal Decree M/33 of 2020), and AI Ethics Principles v2.0 (2023) position Saudi Arabia as one of the more advanced countries in digital governance within the Gulf region.

However, enforcement capacity is only Level 2 (Aware), forming a stark contrast with legislative capacity. Despite enforcement agencies such as SDAIA and NCA possessing extensive powers including suspending data processing, imposing maximum penalties of 5 million Riyals, and initiating criminal prosecutions, actual enforcement activity is almost entirely absent. Since the full PDPL enforcement authority came into effect in September 2024, there are no public records of any violation penalties, and no enforcement cases have been disclosed in cybersecurity and competition regulation.

In terms of leadership in international rules, Saudi Arabia participates in major international standard-setting organizations such as ISO through the Saudi Standards, Metrology and Quality Organization (SASO), but participation is primarily manifested through membership rather than leadership or substantive technical contributions. During its 2020 G20 Presidency, Saudi Arabia demonstrated agenda-setting capacity by prioritizing the digital economy as a theme, but has failed to sustain international digital governance leadership after the conclusion of its G20 Presidency.

Indicator Scores:

3.1 Legislative capacity for digital affairs: Level 3 - Developing

3.2 Enforcement capacity for digital affairs: Level 2 - Aware

3.3 Leadership in international digital technology rules: Level 2 - Aware

3.4 Leadership in international digital behavior rules: Level 2 - Aware

Dimension 4: Digital Capability Independence (2.75/5.0)

The Digital Capability Independence dimension shows significant internal variation, from exceptional strategic coordination (Level 4) to limited research and development output (Level 2) and industrial capabilities (Level 2). Vision 2030 integrates digital technology into 66 out of 99 strategic objectives (67%), representing a globally leading level of coordination. The Saudi Data and Artificial Intelligence Authority (SDAIA) and the National Data Management Office (NDMO) provide systematic oversight mechanisms that surpass the coordination frameworks of most countries. This comprehensive integration views digital technology as infrastructure spanning all development dimensions, rather than as an independent sector.

Talent cultivation demonstrates certain potential (Level 3), with 42% of students in 51 universities pursuing STEM majors, a proportion that is relatively high internationally. Government scholarship programs support students in pursuing advanced STEM degrees in fields such as digital technology, artificial intelligence, and engineering abroad, and the proportion of female participation in STEM education has also increased significantly. However, absolute graduate numbers remain moderate, education quality issues persist, and talent outflow patterns constrain talent retention.

Cutting-edge technology research and development (Level 2) and industry engineering capabilities (Level 2) remain limited. Despite Vision 2030 explicitly prior-

itizing R&D investment, and WIPO patent application data showing growth trends, absolute R&D output is negligible in global comparison. Research is primarily conducted through international cooperation with foreign institutions rather than domestic innovation leadership. Digital technology industry employment and enterprise numbers are growing, but industry engineering capabilities are mainly concentrated in system integration and service delivery rather than product development, with the vast majority of technology companies serving as resellers, integrators, or service providers of foreign technology products.

Indicator Scores:

4.1 Cutting-edge technology research and development: Level 2 - Aware

4.2 Talent cultivation in universities: Level 3 - Developing

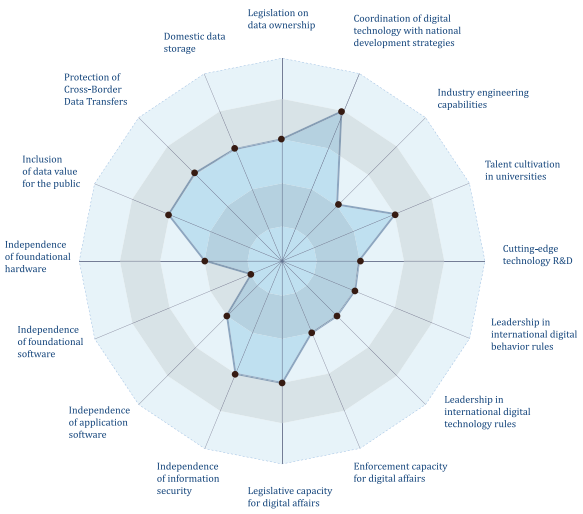
4.3 Industry engineering capabilities: Level 2 - Aware

4.4 Coordination of digital technology with national development strategies: Level 4 - Competent

Summary

Saudi Arabia presents a digital sovereignty landscape where policy architecture far exceeds implementation capacity. The country has successfully constructed the policy and strategic architecture of digital sovereignty—legislative frameworks, institutional structures, strategic coordination mechanisms—but faces the challenging transition toward operational implementation and capability building. The legislative-enforcement temporal asymmetry is a core characteristic: comprehensive regulatory frameworks await enforcement records to demonstrate effectiveness. Infrastructure dependence fundamentally constrains regulatory enforceability—data sovereignty laws are built on a foundation of foreign-controlled technology.

Saudi Arabia's digital sovereignty trajectory depends on translating its strategic coordination advantage (Level 4) into operational outcomes in other dimensions. The country faces a choice between accepting constrained sovereignty within existing dependencies—effective regulation of foreign infrastructure but limited enforcement impact—or making the sustained, expensive investments required for indigenous capability development. Current evidence suggests a hybrid trajectory: continued development of regulatory frameworks while making selective capability investments in priority areas (semiconductors, AI) rather than comprehensive technology stack independence. Whether this partial sovereignty approach can be sustained depends largely on geopolitical factors beyond Saudi control.



Saudi Arabia Digital Sovereignty Index Assessment Results

Dimension Average Scores:

- Dimension 1 - Data Ownership Independence: 3.0/5.0
- Dimension 2 - Digital Infrastructure Independence: 2.0/5.0
- Dimension 3 - Digital Governance Independence: 2.25/5.0
- Dimension 4 - Digital Capability Independence: 2.75/5.0

Indonesia Digital Sovereignty Index Assessment

Assessment Date: October 16, 2025, **DSI Overall Score**: 2.75/5.0 **Country Code**: IDN

Overview

Indonesia's digital sovereignty development presents a significant "scale versus autonomy" paradox: on the one hand, it has achieved remarkable accomplishments in digital infrastructure coverage, economic scale expansion, legal framework construction, and talent cultivation scale, with all four dimensions scoring 2.75/5.0 (Developing) level; on the other hand, it faces systematic structural dependencies in core technology autonomy. The data that best reflects Indonesia's digital strength includes: mobile network penetration exceeding 130%, digital economy market scale surpassing $70 billion (the largest in Southeast Asia), emergence of multiple unicorn companies such as GoTo Group, Bukalapak, and Traveloka, the promulgation of the Personal Data Protection Law (UU PDP) and active enforcement of the PSE registration system demonstrating governance capabilities, and universities graduating thousands of technical graduates annually to support a massive software development industry. These achievements enable Indonesia to reach Level 3 (Developing) in 9 out of 16 assessment indicators, making it one of the more balanced developing countries among BRICS+ nations.

However, this superficial prosperity masks a fundamental sovereignty challenge: Indonesia is completely dependent on foreign suppliers in almost all core technology areas. From network equipment (dominated by Huawei, Ericsson, and Nokia), semiconductors (zero autonomous manufacturing capability), computing hardware (completely imported), to operating systems (monopolized by Windows and Android), databases (dominated by Oracle and MySQL), and other foundational software, Indonesia lacks autonomous production capabilities domestically. R&D investment is less than 0.3% of GDP (far below the 2% international benchmark), and the trade deficit in technology products is massive and continuously expanding. Although the legal framework is comprehensive (with complete legislation in data protection, cybersecurity, electronic transactions, etc.), there are obvious gaps in law enforcement implementation, and coordination among multiple regulatory agencies is fragmented. Engineering capabilities are concentrated at the application layer (e-commerce, fintech, and other consumer-facing services) rather than core technology development and innovation. This "large but not strong" state makes Indonesia's digital sovereignty highly fragile: its scale depends on external technical support, and once supply chains are disrupted or geopolitical changes occur, the entire digital ecosystem may face systemic risks.

Dimension 1: Data Ownership Independence (2.75/5.0)

Indonesia demonstrates a relatively proactive legislative and policy stance in the data ownership dimension, establishing a comprehensive data protection framework through the Personal Data Protection Law (UU PDP, promulgated in 2022), and implementing regulation of foreign platforms through the PSE (Electronic System Operator) registration system, but there remain obvious gaps in implementation enforcement and data value development. Legislation on data ownership (Level 3) is relatively complete, with UU PDP establishing a comprehensive personal data protection framework similar to GDPR, covering core elements such as data processing principles, individual rights, and data controller obligations, and establishing the Personal Data Protection Agency (PDPA) as an independent regulatory body. Together with the Electronic Information and Transactions Law (UU ITE) and Government Regulation 71/2019 (data localization requirements), Indonesia has formed a relatively systematic legal foundation for data governance. However, UU PDP has been implemented for less than three years, enforcement cases and penalty records remain limited, and the independence and resource allocation of regulatory agencies remain to be tested.

Domestic data storage (Level 3) is advanced through Government Regulation 71/2019, which requires electronic system operators (particularly public service providers) to store data domestically in Indonesia and establish data centers. The government enforces compliance by foreign companies through the PSE registration system, with hundreds of foreign platforms having completed registration, including major platforms such as Google, Facebook, and TikTok. However, the physical presence of data centers does not equate to data sovereignty: the hardware, software, and management systems of these centers are almost entirely dependent on foreign technology, and Indonesia has limited actual control over the data. Protection of cross-border data transfers (Level 2) reflects policy awareness but lacks systematic implementation. While regulations require data localization, there is a lack of clear operational frameworks for specific regulatory mechanisms for cross-border data flows, data export approval processes, and cross-border data transfer agreements. Regarding inclusion of data value for the public (Level 3), the government promotes the open data initiative (Satu Data Indonesia), integrating data resources across departments, but the monetization of data as an economic asset, the realization of citizen data rights, and data value sharing mechanisms are still in the exploratory stage, lacking mature practical cases.

Indicator Scores:

1.1 Legislation on data ownership: Level 3 - Developing

1.2 Domestic data storage: Level 3 - Developing

1.3 Protection of cross-border data transfers: Level 2 - Aware

1.4 Inclusion of data value for the public: Level 3 - Developing

Dimension 2: Digital Infrastructure Independence (2.75/5.0)

Indonesia presents a pattern of scale expansion coexisting with technological fragility in the digital infrastructure dimension, with extensive coverage but seriously limited autonomy due to dependence on foreign technology. In terms of independence of foundational hardware (Level 3), Indonesia has built a nationwide telecommunications network with mobile network penetration exceeding 130%, 4G coverage reaching over 90%, and state-owned telecom operators Telkom and Indosat controlling the backbone network infrastructure. The Palapa Ring project invested over $1.5 billion to build a nationwide fiber optic backbone network covering 514 regions across the country, demonstrating the scale of infrastructure construction and national investment. However, the core components of these infrastructures are almost entirely dependent on foreign suppliers: Huawei, Ericsson, and Nokia dominate the network equipment market, submarine cable systems are controlled by international consortia, and Indonesia has almost no domestic capability in the manufacturing and design of critical network equipment. The control of state-owned enterprises is mainly reflected at the operational level rather than the technological level.

The dependence on independence of foundational software (Level 2) is even more severe, as Indonesia lacks advanced chip manufacturing capabilities and domestic computing infrastructure technology. Although there are multiple data center operators and cloud service providers, the servers, storage devices, and network hardware used by these facilities are all dependent on imports, with zero autonomous semiconductor manufacturing capability. Independence of application software (Level 3) is a relatively strong area in this dimension. Indonesia has a massive software development industry, with thousands of computer science graduates entering the labor market annually, and software outsourcing and application development have regional competitiveness. Domestic companies demonstrate innovation capabilities at the consumer service layer such as e-commerce, fintech, and super apps. However, in foundational software areas such as operating systems (monopolized by Windows and Android), databases (dominated by Oracle and MySQL), and development tools, there is almost complete dependence on foreign products, with domestic software capabilities concentrated at the application layer rather than the system layer. Independence of information security (Level 3) is advanced through the National Cyber and Crypto Agency (BSSN). Indonesia has established a cybersecurity emergency response system (ID-CERT), but defense capabilities mainly rely on foreign security products and services, with limited domestic cybersecurity technology R&D capabilities.

Indicator Scores:

2.1 Independence of foundational hardware: Level 3 - Developing

2.2 Independence of foundational software: Level 2 - Aware

2.3 Independence of application software: Level 3 - Developing

2.4 Independence of information security: Level 3 - Developing

Dimension 3: Digital Governance Independence (2.75/5.0)

Indonesia demonstrates proactive legislative stance and regional leadership in the digital governance dimension, but the effectiveness of law enforcement implementation and international influence remain constrained by capacity and resources. Legislative capacity for digital affairs (Level 3) is relatively comprehensive. Indonesia has promulgated the Electronic Information and Transactions Law (UU ITE, 2008 and subsequent amendments), the Personal Data Protection Law (UU PDP, 2022), the Cybersecurity Bill (under deliberation), and other comprehensive legislation covering core areas such as data protection, cybersecurity, electronic transactions, and digital crimes. The legislative process demonstrates a systematic understanding of digital governance challenges, but there are coordination problems in the legal framework, with overlaps and conflicts among multiple laws, and regulatory authority dispersed among multiple agencies (Ministry of Communication and Information Technology, BSSN, PDPA, Financial Services Authority, etc.), lacking a unified coordination mechanism.

Enforcement capacity for digital affairs (Level 3) is reflected through the PSE registration system. Indonesia actively implements regulation of foreign platforms, having blocked non-compliant foreign websites and services, including PayPal (temporarily) and Yahoo. The 2022 ban on TikTok Shop (later lifted) demonstrated Indonesia's willingness to take tough measures against foreign platforms. However, there are problems with the consistency and effectiveness of enforcement: blocking measures are often selective, technical enforcement capabilities are limited (VPN and proxy servers can easily bypass blocks), and fines and penalties for foreign platforms are insufficient to form effective deterrence. Leadership in international digital technology rules (Level 2) is characterized by regional participation but limited global influence. Indonesia, as the rotating ASEAN chair, promotes regional digital governance cooperation and participates in digital agenda discussions in multilateral frameworks such as APEC and G20. However, participation and influence in technical standards organizations such as ITU, ISO, and IEEE are limited, lacking the capacity to lead the formulation of global technical standards. Leadership in international digital behavior rules (Level 3) is relatively strong. Indonesia leverages its population size (280 million) and market position to advocate for data sovereignty principles within ASEAN and regional frameworks, but its voice at the global level remains limited.

Indicator Scores:

3.1 Legislative capacity for digital affairs: Level 3 - Developing

3.2 Enforcement capacity for digital affairs: Level 3 - Developing

3.3 Leadership in international digital technology rules: Level 2 - Aware

3.4 Leadership in international digital behavior rules: Level 3 - Developing

Dimension 4: Digital Capability Independence (2.75/5.0)

Indonesia demonstrates a contradiction between scale and depth in the digital capability dimension, with massive talent cultivation scale but seriously insufficient R&D investment, and engineering capabilities concentrated at the application layer rather than core technology innovation. Cutting-edge technology research and development (Level 2) is the weakest link in this dimension. R&D investment accounts for only 0.3% of GDP (far below the 2% international benchmark, and even further below South Korea's 4.8% and China's 2.4%), with absolute investment scale ranking low globally. Although multiple universities conduct research in fields such as computer science and electrical engineering, research is mainly concentrated at the application level rather than fundamental theory and cutting-edge technology breakthroughs. The number of international academic publications is limited, and high-impact original research results are scarce. The brain drain problem is severe, with excellent researchers and engineers often emigrating to developed countries or being recruited by foreign companies, weakening the accumulation of domestic R&D capabilities.

Talent cultivation in universities (Level 3) is considerable in scale. Indonesia has hundreds of universities offering degree programs in computer science, software engineering, information technology, etc., graduating thousands of students annually. However, education quality is uneven, curriculum content leans toward application skills rather than fundamental theory and innovation capability cultivation, and top talents often choose to study or work abroad. Industry engineering capabilities (Level 3) are relatively strong at the application layer. Indonesia's software development industry has regional competitiveness and can support the development and operation of domestic e-commerce, fintech, super apps, and other platforms. Unicorn companies such as GoTo (merger of Gojek and Tokopedia) and Bukalapak demonstrate Indonesia's capabilities in consumer-facing application development and scaled operations. However, these capabilities mainly rely on foreign technology stacks (cloud services, development frameworks, databases, etc.), and domestic capabilities in core technology component development, system-level engineering, chip design, and other high-end engineering fields are extremely limited. Coordination of digital technology with national development strategies (Level 3) is reflected in the government's formulation of comprehensive digital development strategies such as "Making Indonesia 4.0," emphasizing the integration of digital technology with national development goals, but the consistency and effectiveness of strategy execution are constrained by factors such as departmental coordination, resource allocation, and policy continuity.

Indicator Scores:

4.1 Cutting-edge technology research and development: Level 2 - Aware

4.2 Talent cultivation in universities: Level 3 - Developing

4.3 Industry engineering capabilities: Level 3 - Developing

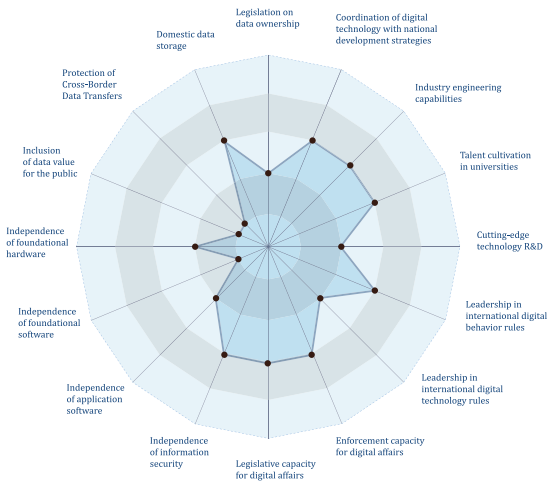
4.4 Coordination of digital technology with national development strategies: Level 3 - Developing

Summary

Indonesia's digital sovereignty status reveals a country at a critical turning point. The DSI overall score of 2.75/5.0 and the consistency of all four dimension scores (all at 2.75) reflect substantial progress in digital infrastructure construction, economic scale expansion, legal framework establishment, and talent cultivation, but also expose a deeper systemic challenge: the fundamental gap between scale and autonomy.

Indonesia's digital sovereignty challenge is not isolated to specific areas but rather a structural dependency problem running through all dimensions. Among the 16 assessment indicators, although 9 reach Level 3 (Developing), not a single indicator reaches Level 4 (Competent) or Level 5 (Independent), reflecting a "ceiling effect" in capability building: excellent performance at the application layer and scale expansion, but difficulty in breaking through in core technology autonomy.

What best reflects this dilemma is the complete external dependence of the technology supply chain: network equipment (Huawei, Ericsson, Nokia), semiconductors (zero manufacturing capability), operating systems (Windows, Android), cloud infrastructure (AWS, Google Cloud, Azure), databases (Oracle, MySQL), and all other critical technology layers are dominated by foreign suppliers. This dependence makes Indonesia's digital sovereignty highly fragile: once supply chains are disrupted, geopolitical changes occur, or foreign platform policies adjust, the entire digital ecosystem may face systemic risks. R&D investment of less than 0.3% of GDP is the fundamental cause of the capability gap. Without sustained large-scale R&D investment, it is difficult to achieve breakthroughs in core technology areas. To move from "Developing" to "Competent" or "Independent" levels, Indonesia needs to achieve fundamental transformations in the following aspects: drastically increase R&D investment (to at least 2% of GDP), emphasize quality rather than just scale in talent cultivation, establish strategic partnerships that genuinely transfer core technologies, formulate coordinated industrial policies focusing on critical technology breakthroughs, and realistically prioritize key areas (it is impossible to achieve breakthroughs in all technology areas simultaneously).



Indonesia Digital Sovereignty Index Assessment Results

Dimension Average Scores:

- Dimension 1 (Data Ownership Independence): 2.75/5.0
- Dimension 2 (Digital Infrastructure Independence): 2.75/5.0
- Dimension 3 (Digital Governance Independence): 2.75/5.0
- Dimension 4 (Digital Capability Independence): 2.75/5.0

Beyond the Multitude: State–Society Alliances as a Strategy Against Big Tech's Digital Hegemony

Published in MGIMO Review of International Relations, citation information:

Xiong Jie. Beyond the Multitude: State–Society Alliances as a Strategy Against Big Tech's Digital Hegemony. MGIMO Review of International Relations. 2025, 18(4): 85-109

In recent years, the digital hegemony dominated by American Big Tech has emerged as a formidable global challenge. A substantial body of scholarship demonstrates that these corporations have not only established economic monopolies but have also, at a socio-cultural level, perpetuated and deepened inequalities and systems of oppression along multiple axes, including race, class, and gender. In response, numerous strands of critical scholarship and resistance movements have arisen in the West. Among them, a particularly influential intellectual current is rooted in the thought of the Italian philosopher Antonio Negri and his long-time collaborator Michael Hardt. This context gives rise to a pressing set of questions: despite being underpinned by a sophisticated leftist theoretical framework, why do these resistance practices—centred on the spontaneous struggles of the "multitude"—consistently prove ineffective in confronting entrenched digital hegemony? And what might constitute a more viable path of resistance?

Critical research on digital hegemony has produced valuable insights. Zuboff (2020) has articulated its underlying economic logic as "surveillance capitalism," while scholars such as Noble (2018), Eubanks (2019), and Benjamin (2020) have empirically revealed how algorithms and big data perpetuate and entrench social injustice. Building on this foundation, authors including Scholz (2013) and Fuchs (2013) have analysed the structural exploitation of "digital labour" embedded within the capitalist system that sustains this hegemony. Yet, with regard to strategies of resistance, much of the prevailing critical discourse has been shaped by the theoretical contributions of Hardt and Negri (2001, 2011), which place their hopes in the capacity of the multitude to reclaim control over the digital commons through decentralised, self-organising struggles—exemplified by initiatives such as platform cooperativism.

This article contends that a significant gap persists in the literature. While these alternative strategies are widely discussed, they have repeatedly failed in practice, and academic debate has not sufficiently interrogated the structural reasons for this recurring failure. More crucially, because Negrian theory rejects the state apparatus a priori, this line of critique systematically neglects the potential role of the state in constructing counter-hegemonic alliances. As a result, the "struggle of the multitude" remains mired in a real-world impasse.

To address this gap, the present study employs a critical literature review. Its aim is not merely to catalogue existing scholarship, but to systematically analyse how the Negrian intellectual tradition—particularly its conceptualisations of strategies of struggle, forms of organisation, and the role of the state—has profoundly shaped Western critiques of digital hegemony. This analysis argues that such influence has ultimately led to a dual impasse, both theoretical and practical. To facilitate this critique, the article draws on the political

theory of Cox (2007), especially his framework describing the dynamic interplay between "Empire," sovereign states, and civil society. This perspective serves as a lens through which to expose the structural power asymmetries confronting Negrian-style resistance.

The central argument of this article is that overcoming Big Tech's digital hegemony requires moving beyond the spontaneist paradigm of the "multitude" as conceived in Negrian theory. While this framework has illuminated important dimensions of inequality and oppression in digital spaces, its reliance on isolated civil society action renders it structurally incapable of confronting the formidable "Empire" coalition formed by the United States state apparatus in alliance with transnational technology corporations. A more viable counter-hegemonic strategy, this article contends, lies in forging robust state–civil society alliances capable of mobilising political, economic, and technological resources at a scale commensurate with the challenge. The analysis concludes by suggesting that, while the European Union's experience provides a useful preliminary reference, China's model of digital governance offers a more compelling example of the successful construction and operation of such an alliance—one that warrants closer scholarly attention and critical evaluation.

The Problem's Roots: The Negrian Framework and Digital Hegemony Critiques

Since 2010, numerous Western scholars have criticised the digital hegemony of Big Tech — almost all of which are American—whose economic scale rivals that of nation-states and whose global influence is profound. These critiques underscore that the digital sphere monopolised by Big Tech reproduces and amplifies entrenched forms of discrimination and oppression within Western, and particularly American, society. Vulnerable groups are disadvantaged across multiple dimensions, including race, ethnicity, gender, sexual orientation, occupation, and income. Such findings have drawn sustained attention from progressive Western scholars and social movements.

The intellectual influence of the contemporary leftist philosopher Antonio Negri, in collaboration with Michael Hardt, is particularly evident in this critical discourse. Their theory of Empire is especially instructive for analysing "capitalist activities that operate directly on a global plane" (Mezzadra & Neilson 2019: 100–101) — a description that aptly captures the operational logic of today's Big Tech. Ross (2013) observed that the work of "commentators of the Italian school" (principally Negri and his associates) on capitalism's control over immaterial labour offers valuable insights into "the new model of capital accumulation represented by Facebook" from a Marxist perspective. Similarly, in his review of Shoshana Zuboff's The Age of Surveillance Capitalism, Morozov characterised Zuboff as "the American heir to Italian Autonomist Marxism" and wryly remarked that "if Negri taught at Harvard Business School, he would sound just like Zuboff". This quip is revealing in its recognition that information technology enables the "Great Other" to exercise pervasive control over the biopolitical production of the "multitude".

Beyond its insights into Empire's totalising control over immaterial labour, several other aspects of the Negrian theoretical tradition have exerted a marked influence on contemporary critiques of digital hegemony.

Consciousness of Contradiction

Negri contends that class contradiction is neither the sole nor the primary contradiction, instead emphasising the multiplicity of social antagonisms. He argues that "no one domain or social organization takes priority over the others… It is no longer possible to lead or even conceive of revolutionary action in a single domain", by which he specifically means that contradictions relating to race, gender, and sexual orientation should be addressed on an equal footing with class and economic contradictions. This position is far from universally accepted among leftist thinkers. Miliband (1985), for example, maintained that "in capitalist society, no other groups, movements or forces are remotely capable of mounting as effective and formidable a challenge to the existing structures of power and privilege as organised labour". Yet he immediately qualified this by noting, "this is not to say… that the women's movement, the black movement, the peace campaigners, the ecologists, the gay movement and

others are of no importance".

Guided by this sensitivity to multiple contradictions, Western — particularly American — critics have been alert to the ways in which the injustices experienced by groups such as Black people and women are exacerbated and reinforced by digital technologies. This perspective has not only drawn considerable interest from Western audiences but has also underpinned a wide-ranging and multidimensional critique of digital hegemony.

Struggle Strategy

Negri consistently champions the spontaneist struggles of the "multitude" and rejects organised forms of conflict. He maintains that "democracy is understood only through democratic action. We must… proceed democratically toward democracy". He also praises Gramsci's concept of the "passive revolution," identifying "peaceful street demonstrations, exodus, media mobilisations, strikes, transgressing gender norms, silence, irony, and the like" as legitimate modes of struggle for the multitude (Hardt & Negri 2011: 363–368). Guided by this philosophy of resistance, Western critics have proposed a diverse array of methods.

Yet, as Amin has observed in his critique of Negri, "all the rebellions of the subaltern—or the multitude—have failed". In a manner almost resembling a self-fulfilling prophecy, the various strategies of struggle advocated by these critics have yielded negligible results: a handful of American Big Tech firms have continued to expand their near-monopoly over the global — excluding China — digital sphere, while the structural injustices identified by their critics show little sign of abating. Struggles conducted without the intervention of powerful institutional actors have, in practice, exerted minimal influence on the entrenched dominance of Big Tech.

Organisational Method

The core reason for Negri's opposition to organised conflict lies in his categorical rejection of all forms of the state apparatus. In his view, "the multitude does not see the state as a realm of freedom but as a den of domination" (Hardt & Negri 2011: 355). He goes so far as to claim that socialists are "nothing but scoundrels" and that leftist leaders "want to be bosses, and since they cannot be bosses in a private capacity, they become bosses in the public capacity of the state" (Negri & Valvola Scelsi 2006: 32–43). Negri further insists that "the objective that Lenin and the soviets posed for an elite, vanguard, insurrectional activity must today be expressed by the desire of all" (Negri & Hardt 2014).

Yet Negri remains notably vague on how this "desire of all" should be organised and translated into concrete political action. Some critics of digital hegemony have sought to employ technological innovations — such as peer-to-peer networks and blockchain systems — as direct instruments for articulating this collective will. However, these initiatives have without exception reached an impasse, failing to mount any substantial challenge to the entrenched digital dominance of Big Tech.

State Participation

Ultimately, Negri adopts a passive and ambiguous stance toward transitional arrangements preceding the achievement of communism. He rejects the common transitional solutions that emerged from the anti-imperialist struggles and national independence movements of the twentieth century — such as socialist and nationalist states—regarding socialism as merely a vehicle for left-wing leaders to "be the boss" under the aegis of the state, without offering any genuine democratic improvement over capitalist society. He characterises the Soviet socialist experience as "a bad memory" (Negri & Valvola Scelsi 2006: 26). In his conceptualization, globalization has reached a stateless stage: imperialism has evolved into a centerless yet omnipresent Empire, rendering obsolete the transitional strategies of confronting imperialism through socialist or nationalist states. Accordingly, the multitude, he argues, should advance "democratically" and directly toward a communist society.

However, as Amin incisively observes, Negri denies that imperialism has a center, yet "the powers that be in Washington are perfectly clear about where that center is". As forty-nine countries in the Global North are increasingly integrated into a unified imperialist bloc under U.S. leadership, for states in the Global South to abandon the option of state-led strategies is effectively to forgo the possibility of development and even the defense of sovereignty — thereby exposing themselves to renewed forms of re-colonization. In the context of efforts by Global South countries to re-

sist the digital hegemony of American Big Tech, the challenge of constructing state capacities capable of countering digital colonialism and reclaiming control over digital technologies from Global North capital has become particularly acute.

This article argues that progressive Western scholars and social movements critiquing contemporary digital hegemony are demonstrably influenced by the Negrian intellectual tradition. This influence equips them to recognize and critique digital hegemony through the lenses of race and gender, but also leads them to avoid, often deliberately, engaging with the role of the state — especially the socialist state — in digital governance. As a result, they fail to meaningfully explore pathways toward dismantling digital hegemony. The predicament of the "struggle of the multitude" with regard to digital hegemony thus serves as a microcosm of the broader dilemma faced by a segment of Western leftist intellectuals, represented by Negri, whose practical strategies of resistance are weak and whose proposals for viable alternatives remain absent.

Consciousness of Contradiction: Comprehending Digital Hegemony Through Multiple Contradictions

In the United States — where political discourse places strong emphasis on identity politics and social diversity — beginning with widely recognised social prejudices relating to race, gender, and other factors can be an effective way to raise awareness of the negative impacts of digital hegemony within American society. Data scientist O'Neil (2016: 23) draws a direct link between racism and digital technology, observing that "racism is the sloppiest of predictive models, driven by messy data collection and spurious correlations, reinforced by institutional inequality, and contaminated by confirmation bias." Given the cognitive limitations of the human brain in acquiring and processing information, "labelling" or stereotyping is a common behavioural pattern. As digital technologies have become deeply embedded in daily life, with data collection and correlation analysis increasingly automated through algorithms and software systems, a critical question arises: has this "sloppy predictive model" been eliminated in the digital age?

Research by American scholars in recent years suggests otherwise. The large-scale application—and frequent abuse—of data and predictive algorithms has not only failed to reduce racial prejudice but has, in fact, reinforced and intensified pre-existing social injustices. For example, in the United States, Black individuals are more likely to be algorithmically classified as potential criminals, charged higher insurance premiums, and denied coverage more frequently (Benjamin 2020). In another instance, a researcher who searched for "black girls" on Google received results dominated by pornographic content (Noble 2018). Comparable patterns affect other ethnic minorities and vulnerable groups: Asian students are more likely to be recommended expensive test-preparation courses, and job advertisements directed toward men display higher salaries than those shown to women. Moreover, studies reveal that low-income groups in the United States—many of whom are people of colour—are subjected to automated, systemic discrimination through "big data policing," facing heightened barriers to accessing social welfare programmes such as housing and healthcare, experiencing restrictions on mobility, and even seeing their children's credit scores negatively affected (Eubanks 2019).

These examples demonstrate that entrenched societal prejudices become deeply embedded within algorithmic systems through the selection and training of data, and subsequently manifest in a variety of ways in digital environments. Without overt malice or the use of derogatory language, and simply by failing to address the biases embedded in historical datasets, it becomes possible to construct a covert, algorithmic analogue of the Jim Crow laws—one that operates seamlessly within the architecture of the digital sphere.

Guided by Negri's emphasis on the multiplicity of contradictions, one can approach the critique of digital hegemony—conceived as an extension of capitalist hegemony—through the lens of identity politics. Marx had long demonstrated that racial antagonism in the Western world has been inextricably bound to the capitalist system from its inception:

Direct slavery is the pivot of bourgeois industry, in the same way that machinery, credits, etc., are. Without slavery you have no cotton; without cotton you have no

modern industry. It is slavery that has given the colonies their value; it is the colonies that have created world trade, and it is world trade that is the pre-condition of large-scale industry. Thus, slavery is an economic category of the greatest importance. (Marx 1976: 167)

Marx (1977: 414) further insisted that the struggle against racism must be understood within the broader struggle of the proletariat: "Labour cannot emancipate itself in the white skin where in the black it is branded." In contemporary society, digital technologies profoundly shape both the productive forces and the relations of production. When the global digital space — excluding China — is effectively monopolised by a small number of American Big Tech corporations, the fundamental contradiction of the capitalist system, that between labour and capital, inevitably manifests in this arena.

As Scholz (2013) notes in the foreword to Digital Labour, the internet "is increasingly turning people into resources for the economic benefit of a few oligarchic owners." The crowdsourcing model of work — later reframed as the "gig economy" — has dismantled full-time employment relationships, fragmenting them into discrete, distributed tasks. This compels workers to compete for lower pay per task, erodes working conditions, and undermines the protection of labour rights (Ross 2013). Platforms such as Uber and Amazon Mechanical Turk separate workers from both the purchasers of their services and from one another, thereby accelerating the decline of traditional forms of unionisation (Srnicek 2021). While workers in some less-developed regions may initially benefit from the new income opportunities such platforms provide, these piece-rate jobs, unprotected by labour legislation, quickly revert to subsistence-level remuneration (Casilli 2017).

As core instruments of Empire's rule, American Big Tech firms go beyond the traditional capitalist exploitation of labour's surplus value. By extracting data value, they turn billions of internet users worldwide into objects of exploitation. Scholars have argued that when users access digital services for "free," their usage behaviour generates vast quantities of data, which constitute a key component of the platform's market value. In this sense, free use is not a gift from the platform but an instance of unpaid labour for it. Users who participate in online discussions (Terranova 2013), fans who create content for their idols (Kosnik 2013), and bloggers who produce regular posts (Dean 2013) all serve as unpaid digital labourers in distinct ways. Even the largest group—users who produce no content but remain addicted to games and social media—are, as Jack Linchuan Qiu (2016) terms them, "iSlaves," trapped by "digital addictive substances" while providing uncompensated labour to platforms. Fuchs (2013) calls this "an extreme form of exploitation," arguing that consumers on digital platforms work entirely without pay, rendering their rate of exploitation effectively infinite. Through their monopoly over digital platforms, Big Tech corporations convert user-generated data from across the globe into proprietary assets.

The value of data lies primarily in its predictive capacity. At the core of machine learning technology is the use of Bayesian statistical methods to predict a user's future behaviour based on historical data. This capability enables digital platforms both to guide and intervene in user behaviour and to employ computer programs that imitate or replace human actions — forming the basis of what is commonly termed "artificial intelligence". The performance of artificial intelligence depends on multiple factors, including algorithmic sophistication and hardware capacity. However, the most decisive factor is the volume of data: the larger the dataset used to "train" an artificial intelligence system, the higher its demonstrated level of "intelligence" and the greater its efficiency and accuracy in performing information-processing tasks traditionally carried out by humans. This relationship is the principal reason data has come to be described as "the new oil".

Operating on the premise that "data is a valuable resource", researchers have emphasised the intrinsic connection between Big Tech's data extraction practices and the capitalist mode of production. Thatcher et al. (2016) argue that the essence of big data lies in dispossessing data from its creators, transforming it into quantifiable user information that can be packaged and sold, and deploying it for the Taylorist disciplining of users—where citizens equipped with smart devices become de facto sensors in the capitalist production apparatus. While mass surveillance was initially justified in the name of counter-terrorism and national security, Big Tech soon discovered that the "behavioural surplus" extracted from such data could generate enormous profits, giving rise to what Zuboff (2020) terms "surveillance capitalism".

In sum, guided by the theory of multiple contradictions

advanced by Negri and other Western leftist philosophers, critics have successfully identified the conflicts between Big Tech and a range of social groups, thereby mapping the contours of digital hegemony under capitalism. In this respect, Negri's thought has offered valuable guidance in constructing the critical problem consciousness necessary for the study of digital hegemony.

Struggle Strategy: The Ineffectiveness of the Spontaneous Struggles of the Multitude

After recognizing that multiple contradictions—including those of ethnicity, gender, and class — were being entrenched and exacerbated in the digital sphere, a range of American scholars and social movements sought to connect these dynamics with the now-mainstream identity politics struggles in the United States and with broader popular protests such as the Black Lives Matter movement. Their aim was, in McIlwain's (2021) words, to "take IT to the streets, and in doing so foment a revolution that would drastically disrupt, shake, or even tear down America's racial order". Notably, these struggles share a defining characteristic: they emphasize peaceful, non-confrontational methods and mobilize civil, non-political forces for spontaneous forms of resistance.

One major category of such efforts focuses on public education to raise awareness about digital technologies and the Big Tech corporations that control them. The Detroit Digital Justice Coalition's DiscoTech ("discovering technology") events, for instance, seek to demystify technology and mobilize communities to question and reshape the "data-driven" decisions that affect their lives. Similarly, the "Our Data Bodies" (ODB) project documents experiences of data-based discrimination from the perspective of marginalized communities. The online magazine The New Inquiry developed an application called White Collar Crime Risk Zones, which ostensibly "uses machine learning to predict where financial crimes are most likely to occur across the US" — a satirical inversion of the algorithmic discrimination routinely targeting people of color and low-income populations (Benjamin 2020).

Other initiatives have targeted specific problems revealed by the deployment of digital technologies. The "Stop LAPD Spying Coalition" is a grassroots campaign opposing the Los Angeles Police Department's use of digital tools to discriminate against and surveil people of color and low-income communities (Eubanks 2019). "Black Girls Code" seeks to equip young African American girls with programming skills, aiming to challenge the exclusion of Black women from Silicon Valley (Noble 2018).

Several organizations have also explored third-party "black box" audits of Big Tech's algorithms. The "Auditing Algorithms" project aimed to cultivate a technically capable community to investigate and evaluate these systems (Benjamin 2020), while the "Non-Aligned Technologies Movement" (NATM) advanced the concept of an "Algorithm Observatory" to identify and expose the harms embedded in Big Tech's algorithmic designs. However, the websites for both initiatives are no longer maintained. The most recent development in this field is the Algorithmic Impact Methods Lab (AIMLab), launched by the Data & Society organization in May 2023. AIMLab's objective is to develop the auditing methodologies necessary to assess the societal impacts of increasingly ubiquitous automated decision-making systems, thereby enabling greater algorithmic accountability. The effectiveness of this initiative remains to be seen.

Some organisations have sought to extend trade unionism into the digital sphere, aiming to organise dispersed gig workers into collective entities capable of defending labour rights against platform-based exploitation. Europe's largest trade union, IG Metall, has pursued this objective through its "Fair Crowd Work" platform, which educates workers about the exploitative conditions in the gig economy. These "digital unions" have achieved occasional successes, such as a 2015 ruling requiring the U.S.-based platform Homejoy to classify its workers as employees, and a 2016 UK court decision obliging the food delivery company Deliveroo to pay the minimum wage (Casilli 2017). However, these victories have been limited in scope, and the overall conditions of gig workers have seen little substantial improvement. In particular, "digitalised" unions have struggled to mount effective challenges against major platforms such as Uber and Amazon. For example, Dynamo — a "quasi-union" spontaneously formed by workers on Amazon's Mechanical Turk —

never amassed more than a few hundred members at its peak and has been inactive since 2020, with its website now defunct.

According to Negri's theoretical framework, the vulnerable groups subjected to oppression across multiple dimensions — race, ethnicity, gender, sexual orientation, occupation, income, and others — collectively constitute the "multitude." The "communicative, collaborative, and affective labour" of the multitude, along with their social life more broadly, form what he terms "biopolitical production". In the postmodern global economy, biopolitical production, rather than industrial factory labour, has become the primary source of wealth creation (Hardt & Negri 2001). Because such production is not simple, repetitive, mechanical work but instead immaterial labour that demands emotional and intellectual engagement, as well as autonomous and responsible collaboration, it inherently fosters unity among the multitude. This unity, in Negri's vision, enables them to reclaim the "commons" through autonomous movements independent of representative systems or vanguard parties. In these movements, the instruments of resistance are not limited to armed struggle but also include "peaceful street demonstrations, exodus, media mobilisations, strikes, transgressing gender norms, silence, irony, and the like" (Hardt & Negri 2011: 363–368). Viewed through this theoretical lens, the struggles outlined above against systemic discrimination in the digital sphere closely align with Negri's conception of resistance.

In practice, however, these non-confrontational, spontaneous struggles have had little substantive impact on the Big Tech corporations that exercise monopolistic control over the digital sphere. While public education campaigns can raise awareness among segments of the population, their influence on corporate behaviour remains minimal. Digital technologies and algorithms are overwhelmingly controlled by a small number of dominant firms, such as Alphabet (Google's parent company) and Meta (Facebook's parent company). The vast power disparity between these corporations and the "multitude" enables them to disregard civil society's demands with near-total impunity.

The fate of earlier initiatives illustrates this dynamic. The "Auditing Algorithms" and "Algorithm Observatory" projects, both designed to scrutinise and hold platforms accountable, received no engagement from Big Tech and ultimately lost momentum. In another case, Yeshimabeit Milner, founder of the "Data for Black Lives" organisation, addressed an open letter to Facebook calling for three specific commitments: anonymising user data and submitting it to a public data trust; collaborating with technical experts and ethicists to create a "Code of Data Ethics"; and hiring Black data scientists and research scientists. As anticipated, Facebook did not respond, and no evidence has emerged to suggest any implementation of Milner's proposals. Two years later, the platform's hate speech detection algorithm still displayed stark racial biases: while antisemitic content was reliably removed, defamatory and racist language directed at Black people and other people of colour frequently remained unpunished.

The persistent failure of such spontaneous, civil-society-led initiatives in the digital space raises a critical question: are these shortcomings the result of contingent factors, or do they reveal deeper, structural causes? This article contends that the latter is the case: these outcomes are rooted in the Negrian intellectual tradition's unrealistic overestimation of direct democracy and its categorical rejection of the role of the state in governance.

Organisational Method: The Dead End of Technology-Based Direct Democracy Attempts

Negri contends that organisational forms such as traditional trade unions and vanguard parties primarily serve the interests of a minority — typically unionised workers. In contrast, he argues, biopolitical production demands a new form of organisation, one that "can overcome all the divisions of the old trade unions and represent the commonality of labour in all its economic, political, and social dimensions," and one "capable of representing every single individual who contributes to the creation of social wealth" (Negri & Hardt 2014). Throughout his works, Negri consistently stresses the imperative of "proceeding democratically toward democracy," advocating that the multitude conduct its struggles through direct democracy rather than relying on any vanguard organisation or state authority. Yet, under the technological conditions of his time, the

mechanisms for realising this vision of direct democracy remained vague — one of the reasons his ideas have frequently been criticised as impractical.

The development of digital technology appeared to offer a potential means of operationalising Negri's vision. With the proliferation of software development tools, cloud computing, and, more recently, blockchain, the question arose: could the general public spontaneously organise to build digital platforms that genuinely served their collective interests? For years, scholars and practitioners have explored the possibility of creating an alternative ecosystem of digital technologies and economic models outside Big Tech's infrastructure, with the aim of fundamentally reshaping labour organisation within the capitalist framework.

More than a decade ago, Bauwens (2013) proposed the creation of "non-capitalist, community-supportive, and use-value-driven entities" to protect and strengthen the commons. His proposed solution was a peer-to-peer (P2P) economy that would connect producers and consumers directly via the internet, eliminating intermediaries such as distributors or employing firms. In Bauwens's view, P2P constituted a viable working model for the new era's labour force, particularly knowledge workers, who would no longer be tied to a fixed workplace but could pursue highly flexible career paths, transitioning "from being hired hands to independent free agents and then entrepreneurs". However, at the time, Uber was only in its infancy, and Bauwens could scarcely have foreseen that the path he envisioned for "using technology to remove the intermediary" would, within a few years, contribute to the emergence of pervasive "cybermediaries" (Jallat & Capek 2001), the "Uberisation" of multiple industries, and the widespread erosion of labour rights in the gig economy.

Costanza-Chock (2020) identifies several strategic approaches to resisting the "Uberisation of everything." Among these, the one that initially attracted the greatest attention was "platform cooperativism," a concept championed by media studies scholar and activist Trebor Scholz and others. This model calls for workers to own and operate their own digital labor platforms — "platform co-ops" — organized as cooperatives but functioning through digital network infrastructures. Since 2014, Scholz and his colleagues have convened an annual conference on platform cooperativism for nine consecutive years, the most recent of which was held in Thiruvananthapuram, the capital of Kerala, India. Around this conference, a global community of practice has emerged; as of February 2024, the Platform Cooperativism Consortium's website listed 548 platform co-op projects across 51 countries.

However, Srnicek (2021) warns that "all the traditional problems of co-ops (e.g., the necessity of self-exploitation under capitalist social relations) become massively exacerbated" in the digital sphere, owing to the monopolistic nature of platforms, the dominance of network effects, and the immense financial and technological resources of incumbent companies. Even if all relevant software were open-source, a platform like Facebook would still be able to mobilize its existing data reserves, entrenched network effects, and substantial capital to repel any cooperative challenger. Put more bluntly, even with the best intentions, emergent platform co-ops must first solve the problem of economic sustainability—a task rendered increasingly formidable by the pervasive dominance of Big Tech monopolies.

These concerns are far from theoretical; they have been borne out in practice. The Green Taxi Cooperative in Denver, Colorado — once the largest taxi company in the city and the second-largest worker cooperative in the United States — was unable to withstand competition from Uber and declared bankruptcy in 2022. Another high-profile example, the music platform cooperative Resonate, has fallen largely silent and faces the likelihood of closure. Although the ten cooperative principles promoted by platform cooperativism, such as "ownership by those who create the value" and "decent pay and income security", remain normatively compelling, building a self-sustaining platform in the shadow of entrenched monopolies is an immense challenge. Without a solid economic foundation, even the most attractive vision risks becoming a castle in the air.

In 2017, the price of Bitcoin surged from just over $900 to nearly $20,000, fueling a speculative boom in digital cryptocurrencies and inspiring new possibilities for platform cooperatives struggling with chronic financial fragility. At the 2018 Platform Cooperativism conference in Hong Kong, the project Musicoin presented its model of paying musicians directly in a blockchain-based cryptocurrency, thereby circumventing exploitation by monopolistic platforms. At its peak, the value of Musicoin's cryptocurrency rose to 119 times its initial issue price. In the years that followed,

more blockchain-based platform co-ops emerged. While the dominant narrative framed blockchain as a tool enabling Decentralized Autonomous Organizations (DAOs) and distributed cooperatives, a significant driver of this proliferation was the rapid appreciation of many cryptocurrencies—mirroring Bitcoin's trajectory — which brought substantial financial windfalls to their issuers. When the cryptocurrency bubble deflated, enthusiasm for "blockchain-based platform co-ops" similarly diminished.

A retrospective look at more than a decade of initiatives—from P2P networks to platform cooperativism — reveals a clear preference among advocates for "self-organization." Hardt and Negri argue that because biopolitical production has supplanted traditional industrial production as the dominant mode of production, the methods by which the multitude resists capital must also adapt. They emphasize the design of mechanisms and frameworks that can democratically resolve conflicts within the multitude, rather than relying on the leadership of a Leninist-style vanguard: "when the technical composition of labor has changed so profoundly, any proposal for a vanguardist political composition is, in the best of cases, anachronistic" (Hardt & Negri 2011: 350–352). Technological innovations such as P2P networks, mobile internet, cloud computing, and blockchain have made the creation of decentralized, self-organizing democratic structures theoretically possible.

In practice, however, multiple waves of attempts to build alternative digital systems for the multitude have failed to produce meaningful results. These democratically oriented, spontaneously organized movements — lacking secure political and economic foundations — face opposition from adversaries with state-level economic capacity and political influence. The experience of the past decade suggests that the former has yet to devise a viable strategy for challenging the entrenched monopolistic hegemony of the latter.

Continuing along this path of democratic, spontaneous innovation, Tim Berners-Lee, inventor of the World Wide Web, has sought to use decentralized technology to dismantle Big Tech's monopoly over data. His proposed solution, Solid, enables users to extract their personal data from web platforms and store it in software or devices called "Pods." Users may then grant platforms permission — potentially in exchange for payment — to access this data, thereby retaining control and benefiting directly from its use. Mhlambi (2020) argues that this approach resonates with the African concept of Ubuntu: users voluntarily contribute data to train artificial intelligence for the benefit of the entire community, without transferring it directly to Big Tech. Yet Solid has encountered challenges similar to those faced by platform cooperativism. Big Tech has ignored Berners-Lee's vision entirely; no major monopolistic digital platform supports Solid, much less seeks users' permission to access data through it. As in the case of Facebook's response to potential competitors, a platform that can crush opposition through its monopoly has no incentive to cooperate — let alone to surrender its most valuable asset.

In sum, over the past two decades — ranging from P2P initiatives to blockchain projects, from platform cooperativism to Solid — a segment of technically skilled practitioners has conducted successive experiments in direct democracy, seeking to build alternative digital solutions capable of attracting large user bases and thereby challenging the dominance of Big Tech. Yet these initiatives have failed to exert any meaningful influence on monopolistic digital corporations; most have struggled simply to survive. It must be acknowledged that when Big Tech commands economic resources on a scale comparable to that of a nation-state and exercises enormous influence over public opinion—shaping, and in some cases even affecting, political processes—the spontaneous organization of the populace faces formidable structural obstacles in creating viable competing platforms. Regulating Big Tech, therefore, is highly likely to require the mobilization of state power.

In Cox's (2007) political theory, Empire — the singular hegemonic position of the United States and the hard and soft power that sustain it — alongside the sovereign state in the Westphalian sense and civil society together comprise the prevailing configuration of global power. These three forces are not independent entities; rather, they intersect, overlap, and at times merge. Alliances between any two—whether temporary or long-term—generate new power configurations that shape both the construction and governance of digital space. If one fails to grasp the dynamic interplay among these forces, and instead frames Empire and the "multitude" organized as civil society as fixed, opposing poles, one cannot adequately conceptualize a viable strategy for dismantling digital hegemony.

State Participation: Rejecting State Involvement in Building Digital Space

As summarized in the preceding section, the solution advocated by many critics of digital hegemony is to mobilize the power of the "multitude" to effect change through bottom-up action. In practice, such initiatives have succeeded in raising public awareness — particularly in the West — about the nature and harms of digital hegemony. However, they have largely failed to alter the underlying structures of power. Faced with the dual challenge that Big Tech has little incentive for self-reform and that alternative technological solutions struggle to survive in market competition, some scholars have emphasized the importance of involving the state and government in addressing this issue.

State participation in shaping the digital sphere can take various forms, differing in their depth of intervention. A more limited form involves legislating and regulating the conduct of businesses operating in digital markets. A more expansive approach entails formulating industrial policies to guide the development of the digital sector or even engaging directly in digital infrastructure through state-owned assets and enterprises. The former model aligns with the liberal conception of the state as a "night-watchman" and is generally preferred by Western countries. The latter is more frequently criticized — often labelled "socialism" or described as "the state advancing as the private sector retreats" — and continues to be viewed with suspicion by a segment of Western left-wing scholars, notably Negri. In practice, however, Western states acting as "night-watchmen" in their regulation of Big Tech have not achieved notable success. For countries in the Global South, which are latecomers and structurally disadvantaged in the fields of information and digital technology, domestic digital spaces are already dominated by a handful of American Big Tech firms; in such circumstances, legislation alone is manifestly insufficient to counter entrenched digital hegemony.

Madden et al. (2017) note that consumer privacy protections in the United States remain markedly weaker than those under the European Union's General Data Protection Regulation (GDPR) of 2016, and legislative progress has been sluggish. The primary reason lies in the United States' stronger "emphasis on individual liberty and corporate innovation." In other words, in the legislative calculus, the "personal dignity" of consumers ranks below the protection of corporate interests—especially those of Big Tech. This situation persists to the present. The prospects for the American Data Privacy and Protection Act (ADPPA), intended to rival the GDPR as a global de facto standard, remain uncertain. At the state level, efforts such as those by Maine State Representative Maggie O'Neil — who sought to enact stricter data privacy legislation — have been blocked by private sector opposition. Her criticism that Big Tech firms "write their own laws" in order to "use our data as they please" encapsulates the structural legislative impasse that characterizes U.S. data privacy policy.

Paradoxically, a 2011 McKinsey research report on the era of big data also recommended legislation to protect user privacy—on the grounds that such regulation would strengthen user confidence and thereby enable companies to collect even more data. In other words, even if the United States were to pass the ADPPA, as Madden et al. (2017) have advocated, the monopolistic hold of Big Tech over data would remain largely unchallenged. Zuboff (2020) likewise observes that despite Europe's more advanced privacy and data protection legislation, and its comparatively stronger anti-monopoly stance, companies such as Facebook and Google operate with equal impunity there. Given the structural reality that Europe lacks internet firms capable of competing with American Big Tech, this outcome is unsurprising.

Srnicek (2021: 70) further acknowledges that even if the state were to regulate Big Tech's monopolistic practices, labor exploitation, and privacy violations, such measures would be "unimaginative and would have very little effect" unless they addressed the underlying structural conditions. He therefore proposes that the state invest resources in building publicly owned and controlled internet platforms, treating them as a public utility. Yet a review of global critical scholarship on digital hegemony reveals that proposals for "state-led digitalization" are rare; and where they do appear, they are often mentioned only briefly and without substantive elaboration. The dominant tendency in this body of work is to emphasize the agency of the "multitude" while largely neglecting the role of the state—an omission that is analytically significant.

Couldry and Mejias (2019) contend that the state's interest in digitalization stems solely from its desire to "exercise surveillance powers to intimidate its citizens or to damage their interests in more subtle ways."

This deep-seated suspicion of all forms of state power aligns with the position of Hardt and Negri (2011: x, 164–165), who argue that the state operates by constructing and reinforcing the national identity of "the people," thereby undermining the commonality of the multitude. Within the capitalist social systems of Europe and the United States, such concerns about the state's coercive and ideological functions are not without merit. Yet, when confronted with Big Tech — an industry deeply embedded in the core of the capitalist state's power — reform movements that cannot secure state support inevitably reach an impasse.

According to Lenin's analysis, imperialism represents the "highest stage of capitalism," in which monopoly organisations mature within Western capitalist states and expand globally, competing for markets through colonialism. This expansionary logic is now being replayed in the digital domain. In their critique of ubiquitous computing, Dourish and Mainwaring (2012) note that the development and dissemination of digital technology reproduces a Wallersteinian "core–periphery" structure: technologies created in industrialised Western countries—particularly the United States—are uncritically transplanted into the developing states of the Global South. In this context, "development" for the Global South entails replicating Western technological applications wholesale, effectively opening domestic digital spaces to Big Tech and enabling the unilateral extraction of data resources.

Facebook's Free Basics initiative in the Global South, especially in Africa, illustrates this dynamic. While presented as a means of providing free internet access, it has been shown to function as a large-scale system for data extraction and digital experimentation (Nothias 2020) — akin to the railways constructed by former colonial powers in their territories for the purpose of transporting mineral resources. It is no coincidence that much of the infrastructure linking the digital space of the Global South—servers, data centres, and submarine cables—follows the same colonial routes established centuries ago, creating vertical connections between periphery and imperial core. Within this infrastructural framework, data exchanges between Asia and Africa must pass through the United States, delivering the "behavioural surplus" to American Big Tech firms (Couldry & Mejias 2019).

From a Global South perspective, Kwet (2019) observes that American Big Tech monopolises the entire industrial chain of data collection, transmission, storage, analysis, and use—from hardware to software to so-called "cloud computing". "As with typical colonialism", he writes, "data is also exploited as a raw material by imperialist powers". Because there are no universally accepted accounting standards for valuing data assets, the precise economic value extracted from the Global South through the colonial appropriation of "data minerals" remains unknown. Nevertheless, the World Economic Forum estimates that, as of 2022, the digital economy accounts for over 15% of global GDP—more than USD 15 trillion. Even using this as a conservative baseline, the annual value of uncompensated data appropriated from the Global South by American Big Tech could plausibly reach hundreds of billions, and potentially even one trillion U.S. dollars. This underscores the urgent need for rigorous, quantitative analysis of this economic phenomenon.

In 1979, Mustapha Masmoudi, then Tunisian Minister of Information and later a member of UNESCO's MacBride Commission, observed: "There is an appalling imbalance in the flow of news and information between the North and the South, an imbalance where the flow from the developed countries to the developing world is enormous, while the reverse flow is minuscule" (Masmoudi 1979). In the age of the internet and digitalisation, this imbalance has taken on new dimensions. News and information still flow predominantly from developed countries to the nations of the Global South, but now data — an increasingly valuable asset — flows in vast quantities from the Global South to developed countries, especially to a handful of data technology giants in the United States.

South Africa, one of the more developed states in the Global South, offers a telling example. It has 45.34 million active internet users (70.8% of the population) and 26 million active social media users (40.6%). Among the twenty most visited websites in South Africa, eleven belong to American Big Tech firms, accounting for 86.4% of total web traffic; South Africa's own websites account for only 5.4%. Six of the ten most popular smartphone applications in the country are American, with only one — developed for Capitec Bank—originating locally. Yet Capitec's information systems run on Microsoft Azure and Amazon AWS cloud services, meaning that its data is also stored and processed under the control of American Big Tech.

In reality, outside the United States — and particularly

in the Global South—rejecting state involvement in the governance of digital space would amount to enacting a form of digital "shock therapy", delivering the vulnerable digital markets of these countries directly into the hands of American Big Tech, which already maintains a position of overwhelming monopoly. Unsurprisingly, this position aligns with the view of the World Economic Forum: "governments just need to be able to access company-owned data remotely; it does not matter where the data is stored". In practice, this prescription perpetuates the status quo in which the overwhelming majority of Global South states hand over control of their data to U.S. technology corporations.

As Schiller (1992) noted more than fifty years ago, in circumstances where the United States possesses absolute technological superiority, the doctrine of "free flow of information" — which denies weaker nations the right to regulate the movement of information — functions as "a channel for imposing a way of life and values on weaker nations". Yet, as previously noted, most Western researchers — working in the intellectual lineage of Negri — lack confidence in the state under capitalism (a category encompassing most Global South countries) and remain unwilling to envisage state power as a legitimate instrument for the governance of digital space.

As Harvey (2009) argues in his critique of Commonwealth, "[subverting the existing structures of capitalism and providing an alternative one] is too great a task for a flat, self-organising movement of autonomous beings to accomplish", and "their argument offers no concrete strategy for… the revolutionary transformation of the material basis of everyday life". This criticism aptly captures the predicament confronting the various spontaneous struggles of the multitude in the digital sphere. From denouncing Facebook's racial discrimination to attempting third-party audits of Big Tech algorithms; from exposing the extraction of data resources and appropriation of behavioral surplus to experimenting with technologies like Solid to return personal data to users; from P2P networks to platform cooperativism — none of these efforts have significantly dented Big Tech's hegemonic power.

Their repeated setbacks are not accidental but systemic and rooted in theory. The categorical rejection of any form of sovereign state participation in the construction and governance of digital space has left such movements structurally incapable of mounting a serious challenge. In this sense, a discourse and practice that excludes the state has, paradoxically, become complicit in sustaining Big Tech's dominance, reinforcing the perception — time and again — that the status quo is immutable.

As previously discussed, disregarding the role of the sovereign state within the current global configuration of political power—and expecting the "multitude" or civil society to confront the "Empire" single-handedly — constitutes a theoretical flaw that has left many Western researchers in a conceptual dead end when seeking strategies to dismantle American digital hegemony. A frequent phenomenon in the Global South is the convergence of American Big Tech — a key pillar of the U.S. tech–military–intelligence complex and thus a concrete embodiment of Empire — and segments of civil society (often NGOs) in jointly rejecting state involvement in the governance of digital space. A telling example is Google's $300 million "investment" in Latin America to "provide economic opportunities and digital skills training to NGOs", of which $250 million consisted of credits redeemable only for Google advertising. This is a classic case of Empire and civil society collaborating to obstruct sovereign state efforts to strengthen domestic digital infrastructure and governance capacity. In such a context, the portion of civil society that has not been co-opted by Empire must form an alliance with the third vertex of the power configuration—the sovereign state—if there is to be any realistic prospect of jointly confronting imperial hegemony.

In this regard, Dean (2019) critiques Negri's vision as "a platform for demands with no vehicle, no substance — Then who is to make the demand?" She adds that "as we learned from Lenin… without the leadership of the Party, it is very difficult for the people to see the situation clearly… Their actions are co-opted and diverted, channeled and packaged to support the system they oppose." It is not difficult to envision that in non-socialist, non-communist-led countries—such as India or Brazil—a social-democratic government should assume the responsibility of allying with and guiding the "multitude". Kavada (2019) advances a complementary strategy of "appropriating the capitalist digital machine": imposing taxes on global internet giants and compensating the public for their unpaid digital labor on online platforms through a universal basic income. Such a policy could create a resource base for alternative digital solutions, including platform cooperatives and P2P production. Crucially, Kavada stresses that to

realize such strategies, the Left can no longer "be afraid of… state power," as any alternative developed without the state's support will remain marginalized and economically unsustainable.

Conclusion

It is perhaps no coincidence that among the dozens of scholars critically examined in this article, none could be described as Luddites advocating the abandonment of the internet and a return to a pre-digital era. Given that ceasing the large-scale use of smartphones and social networks is not a viable option, there are essentially only two conceivable paths forward: either to regulate existing (and future) Big Tech firms so that they serve, rather than harm, the broadest segments of the population; or to build alternative digital platforms and, from the standpoint of ownership, ensure that such platforms do not revert to the familiar capitalist trajectory.

After considering the unsuccessful experiences of platform cooperativism, the Non-Aligned Technologies Movement, Solid, and other attempts to create alternative digital platforms, Srnicek's concern about whether such initiatives can survive in a capitalist environment appears all the more prescient. Moreover, the vast majority of these alternative platforms have been organized as enterprises; if they were to grow to the scale of hundreds of millions of users, there is no structural mechanism within capitalism to guarantee that they would remain faithful to their founding principles rather than evolving into another iteration of Big Tech. As Fuchs has observed, digital hegemony is essentially the projection of the capitalist system into the digital realm, and any fundamental solution must therefore seek to transform the underlying social system. This raises a crucial question that deserves far greater scholarly attention: what would a socialist, publicly owned — or at least publicly beneficial — digital platform look like?

According to the "Digital Dependency Index" published by the University of Bonn, China is the only country other than the United States to possess a relatively independent information infrastructure. All other states must rely on foreign-owned platforms and related technologies for their digital activities, with most economies almost entirely dependent on foreign platforms — overwhelmingly those of U.S. origin (Mayer & Lu 2023). In contrast to the vision promoted by Big Tech, the Davos elite, and the authors of Commonwealth — who depict cyberspace as a "global common" existing beyond national sovereignty — the Chinese government has consistently treated cyberspace as a natural extension of its sovereign territory. In 2007, then-President Hu Jintao, during a collective study session of the CPC Central Committee Politburo, first introduced the expression "cyberspace" and proposed "to make the internet a new channel for disseminating advanced socialist culture, a new platform for public cultural services, and a new space for the healthy spiritual and cultural life of the people". This formulation clearly continued Deng Xiaoping's principle, articulated at the 14th National Congress of the CPC (1992), of "grasping with both hands, and keeping both hands firm" in the development of material and spiritual civilization: the online world is not an autonomous realm independent of the material world, but an extension of physical space, and thus falls firmly within the scope of state sovereign control. Since the 18th National Congress of the CPC (2012), the new generation of national leadership under Xi Jinping has repeatedly emphasized that "the internet is not a lawless place," reaffirming this conceptual approach. Compared to the recommendations of the World Economic Forum, this conception of cyberspace more closely reflects the position and priorities of the Global South.

Against this backdrop, discussion among global critics of American Big Tech's digital hegemony regarding China's experience in building and governing its digital space is strikingly limited — if not entirely absent. This general silence is noteworthy. Mejias (2020) asserts that China — like the United States — is "another power center of data colonialism". Fuchs (2015) likewise contends that "commercial and profit-driven logic dominates the Chinese internet and Chinese social media, just as it dominates the American internet". Jack Linchuan Qiu (2016) describes how Foxconn in China and Apple in the United States form an alliance within the broader framework of the global capitalist system, transforming both workers and consumers into "iSlaves". Such perspectives — framing Chinese digitalization as essentially no different from that of the United States — may have contributed to the reluctance of many critics to consider the Chinese experience as a potential model for countering the digital hegemony of American Big Tech.

Lü Xinyu (2018) recalls that China's internet sphere in the 2000s was initially controlled and embedded within global hegemony — particularly through the persistence of Cold War discourse into the post–Cold War era. Following the strict containment of attempted Western-style "colour revolutions", the sphere evolved into one dominated by the market and by data monopolies established by domestic Big Tech firms such as Baidu, Alibaba, and Tencent (collectively known as BAT) — the same "commercial and profit-driven logic" identified by Fuchs. However, a significant turning point came with the 2016 Speech at the Symposium on Cybersecurity and Informatisation Work, which set a political ceiling on the activities of Chinese internet enterprises. The government explicitly required that the development of the internet and informatization "must implement a people-centered development philosophy". In the years since, under this policy framework, the Chinese state has implemented a series of regulatory measures and policy guidelines directed at its Big Tech sector, addressing in concrete terms several of the harms of digital hegemony outlined earlier in this article.

Is China constructing the "alternative internet under an alternative model of social relations" that Fuchs envisions? Answering this question requires sustained theoretical and empirical investigation — far beyond the scope of this article. Yet at least phenomenologically, it is observable that over the past decade, the Chinese government (and the ruling party) has forged an alliance with its population — though not necessarily in the form of "civil society" as understood in the Western context — to counter the digital hegemony of the Empire, achieving notable results. These cases, and the theoretical insights they offer into the current configuration of global power, merit careful attention from researchers.

References

Bauwens M. 2013. Thesis on Digital Labor in an Emerging P2P Economy. Scholz T. (ed.). Digital Labor: The Internet as Playground and Factory. Essay, New York: Routledge.

Benjamin R. 2020. Race after Technology: Abolitionist Tools for the New Jim Code. Cambridge: Polity.

Casilli A. 2017. Digital Labor Studies Go Global. International Journal of Communication. №11. P. 3934–3954.

Costanza-Chock S. 2020. Design Justice: Community-Led Practices to Build the Worlds We Need. Cambridge, Massachusetts: The MIT Press.

Couldry N. and Mejias U.A. 2019. The Costs of Connection: How Data is Colonizing Human Life and Appropriating It for Capitalism. Stanford, California: Stanford University Press.

Cox R.W. 2007. 'The International' in Evolution. Millennium: Journal of International Studies. 35(3). P. 513–527. DOI: 10.1177/03058298070350030901

Dean J. 2013. Whatever Blogging. Scholz T. (ed.). Digital Labor: The Internet as Playground and Factory. Essay. New York: Routledge. P. 162–188.

Dean J. 2019. Critique or Collectivity? Communicative Capitalism and the Subject of Politics. Chandler D. and Fuchs C. (eds). Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data. Essay. London: University of Westminster. P. 171–182.

Dourish P. and Mainwaring S.D. 2012. UBICOMP's Colonial Impulse. Proceedings of the 2012 ACM Conference on Ubiquitous Computing.

Eubanks V. 2019. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York, NY: Picador.

Fuchs C. 2013. Class and Exploitation on the Internet. Scholz T. (ed.). Digital Labor: The Internet as Playground and Factory. Essay. New York: Routledge. P. 263–279.

Fuchs C. 2015. Baidu, Weibo and Renren: The Global Political Economy of Social Media in China. Asian Journal of Communication. 26(1). P. 14–41. DOI: 10.1080/01292986.2015.1041537

Hardt M. and Negri A. 2001. Empire. Harvard University Press.

Hardt M. and Negri A. 2011. Commonwealth. Cambridge, Massachusetts: Harvard University Press.

Harvey D., Hardt M. and Negri A. 2009. Commonwealth: An Exchange. Artforum. 48(3).

Jallat F. and Capek M.J. 2001. Disintermediation in Question: New Economy, New Networks, New Middlemen. Business Horizons. 44(2). P. 55–60. DOI: 10.1016/S0007-6813(01)80023-9

Kavada A. 2019. The Movement Party – Winning Elections and Transforming Democracy in a Digital Era : Reflections on Paolo Gerbaudo's Chapter. Chandler D. and Fuchs C. (eds). Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data. Essay. London: University Of Westminster. P. 199–204.

Kosnik A.D. 2013. Fandom as Free Labor. Scholz T. (ed.). Digital Labor: The Internet as Playground and Factory. Essay. New York: Routledge. P. 123–142.

Kwet M. 2019. Digital Colonialism: US Empire and the New Imperialism in the Global South. Race & Class. 60(4). P. 3–26. DOI: 10.1177/0306396818823172

Lü X. 2018. “Archaeologies of the Future” in the New Media Era: The Reform of Chinese Media in the Perspective of Communication Political Economics. Journal of Shanghai University (Social Sciences Edition). 35(1). P. 121–140.

Madden M., Gilman M., Levy K., et al. 2017. Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans. Washington University Law Review. 95(1). P. 53–125.

Marx K. 1976. The Poverty of Philosophy. Marx–Engels Collected Works. Essay. New York: International Publishers.

Marx K. 1977. Capital: A Critique of Political Economy. New York: Penguin.

Masmoudi M. 1979. New World Information Order. Journal of Communication. 29(2). P. 172–179.

Mayer M. and Lu Y.-C. 2023. Digital Autonomy? Measuring the Global Digital Dependence Structure. SSRN Electronic Journal. DOI: 10.2139/ssrn.4404826

McIlwain C.D. 2021. Black Software: The Internet and Racial Justice, from the AFRONET to Black Lives Matter. New York: Oxford University Press.

Mezzadra S. and Neilson B. 2019. The Politics of Operations: Excavating Contemporary Capitalism. Durham: Duke University Press.

Mhlambi S. 2020. From Rationality to Relationality: Ubuntu as an Ethical and Human Rights Framework for Artificial Intelligence Governance. Carr Center Discussion Paper Series. №9.

Miliband R. 1985. The New Revisionism in Britain. New Left Review. №150.

Negri A. and Hardt M. 2014. Multitude: War and Democracy in the Age of Empire. New York: Penguin Books.

Negri A. and Valvola Scelsi R. 2006. Goodbye Mr. Socialism. Milano: Feltrinelli.

Noble S.U. 2018. Algorithms of Oppression: How Search Engines Reinforce Racism. New York: New York University Press.

Nothias T. 2020. Access Granted: Facebook’s Free Basics in Africa. Media, Culture & Society. 42(3). P. 329–348. DOI: 10.1177/0163443719890530

O’Neil C. 2016. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York: Crown.

Qiu J.L. 2016. Goodbye iSlave: A Manifesto for Digital Abolition. Chicago: University of Illinois Press.

Ross A. 2013. In Search of the Lost Paycheck. Scholz T. (ed.). Digital Labor: The Internet as Playground and Factory. Essay. New York: Routledge. P. 13–32.

Schiller H.I. 1992. Mass Communications and American Empire. Westview Press.

Scholz T. 2013. Introduction: Why Does Digital Labor Matter Now? Scholz T. (ed.). Digital Labor: The Internet as Playground and Factory. Essay. New York: Routledge. P. 1–9.

Srnicek N. 2021. Platform Capitalism. Malden, Massachusetts: Polity Press.

Terranova T. 2013. Free Labor. Scholz T. (ed.). Digital Labor: The Internet as Playground and Factory. Essay. New York: Routledge. P. 44–75.

Thatcher J., O'Sullivan D. and Mahmoudi D. 2016. Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data. Environment and Planning D: Society and Space. 34(6). P. 990–1006. DOI: 10.1177/0263775816633195

Zuboff S. 2020. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs.

Institutional Profiles

Global South Academic Forum

The Global South Academic Forum is an international research collective rooted in the Global South Research Center at the International Communication Institute of East China Normal University. The Forum focuses on developing theoretical frameworks for digital sovereignty that address the specific technological and geopolitical realities of developing nations. By pioneering the Digital Sovereignty Index (DSI), the Forum provides an intuitive measurement system for national independence and serves as a vital platform for dialogue and cooperation among Global South countries.

Institute for Digital Economy and Artificial Systems (IDEAS)

The Institute for Digital Economy and Artificial Systems (IDEAS) is a global academic platform dedicated to the digital economy, AI, and international trade. Through its specialized centers, including the Center for South Asia & Middle East Studies, IDEAS facilitates high-level research and scholarly content creation to safeguard national development rights. As the academic and publishing partner for the DSI Report, IDEAS ensures the integration of Global South research into the international scholarly ecosystem through its partnership with Wiley and highlevel forums like the Zhongguancun Forum.