

*The rapid advances in digital and AI technologies have the potential to reshape the digital landscape and redefine notions of sovereignty, requiring nations to adapt their policies, regulations, and strategies to navigate the opportunities and challenges presented by AI-enabled future.*

The point of departure for this concept note must be the acknowledgement of the fact that UN Member States (MSs) have been negotiating the Global Digital Compact (GDC) which is to be adopted at the Summit of the Future in just a matter of days.

The stated goal of the DGC is to “promote an open, free, secure, and human-centric digital future.” At the heart of the GDC is the call for urgent multi-stakeholder cooperation across domains, governmental and non-governmental, public and private. There are two stated main rationales and imperatives for the GDC: (1) to bridge the digital, data, and innovation divides, and (2) to establish the governance required for a sustainable digital future. (See “*Our Common Agenda policy brief #5*”).

The GDC - as is the case with the overall paradigm behind the United Nations-driven “global agenda for change” - has implications for MS’s sovereignty; it presupposes and calls for MSs accepting “dispersed sovereignty.” In order to achieve collaboration towards the goal of a truly “global,” “common” and “open” future, MSs are expected to curtail and open-up their sovereign jurisdictions in order for the universal goals and objectives to have a chance of being achieved.

Sovereignty embodies a legitimate and controlling authority, akin to the captain of a ship, drawing from Plato's cybernetic analogy of “steering” the ship. The ongoing discourse surrounding its exercise, by whom, in what manner, and for what objectives, has significantly influenced the course of modern history, ever since the Westphalian conceptualization of the nation state and its sovereignty, to more recent conceptualizations of sovereignty in the multilateral age centered around the United Nations.

However, our era primarily constitutes the digital age. Within this digital landscape, the “infosphere” transcends physical boundaries; data, unlike natural commodities, are not finite, scarce, or rivalrous, but instead, digital assets are predominantly private and influenced by market dynamics. Furthermore, citizens’ personal profiles are not only shaped by states but also by globalized multinational corporations. **Consequently, the digital age compels states to reassess the concept of sovereignty.** While traditional formal sovereignty remains essential, it is increasingly inadequate, much like the role of the State itself. **Therefore, new conceptualizations of contemporary digital sovereignty are imperative to establish effective and democratic forms of control through appropriate regulation. However, the question arises: who should wield such sovereignty, both in practice and in principle?**

This question is especially pertinent in the light of the fact that much of the digital sphere is under the ownership and prerogative of private corporations and the information technology ecosystems within which they operate and dominate. It is an established fact, for instance, that the bulk of big data and pools of information, on which key digital platforms and Artificial Intelligence (AI) depends, are not owned by governments but rather the technology giants such as Google, Facebook, Amazon, Alibaba, Baidu, etc. **And since AI relies heavily on data, the ability to collect, analyze, and control data becomes crucial for nations' sovereignty and, potentially even, their peace and security.**

However, while these entities are powerful and agile in bringing to market new applications and technologies, the real point is that, between companies and states, **“the former can determine the nature and speed of change, but the latter can control the direction of change.”** Thus, the state can exercise digital sovereignty intrastate as well as interstate.

**The notion of digital sovereignty, in the face of present dynamics in the socio-economic and geopolitical domains, calls for pragmatically balancing, on the one hand, universally dispersed sovereignties (so that noble and highly beneficial multilateral initiatives, such as the GDC, could be successfully pursued) with the need, on the other hand, to strengthen national and supranational digital sovereignties.**

This proposition for balancing models of sovereignty becomes imperative and perhaps even inevitable when one considers the great power competition that is undeniably on the rise. Stated differently, the emergence of a “multipolar world” in geopolitics with major inherent implications for global governance, including governance of the digital sphere, strongly recommends the proposition for a pragmatic balancing of (1) dispersed and (2) concentrated sovereignties.

A credible and compelling argument could be made that such an approach is particularly relevant for consideration by the Global South, most of whose states do not have the capital and the technology to invest in robust digital capabilities and AI applications. **The Global South countries are already and will increasingly be confronted by the crucial question of whether and to what extent they are likely to experience a diminishment of their respective political and national sovereignty as a consequence of losing digital sovereignty, either to multinational corporations or foreign governments.**

The fact is that while the UN is spearheading the process towards GDC - which is predicated upon openness, trust, and collaboration by all parties - several digital/AI governance ecosystems have been emerging, which can only be characterized as **efforts to assert digital sovereignty**. The four big ones are:<sup>1</sup> (1) the EU via the recently adopted “AI Act,” (2) the OECD, which hosts a Global Partnership on AI within the stated jurisdiction of OECD countries, (3) USA via its emerging multifaced AI governance structure, and (4) China’s own AI governance framework. The context in which these regional/national governance ecosystems are being formulated is one of **growing ideological differences, great power competition and the emergence of a multipolar world**. It’s highly possible that these ideological differences between the great tech powers could have broader geopolitical consequences for managing the digital sphere, AI and information technology more broadly in the ensuing months and years. Control over digital strategic resources, including data, software, and hardware, has become paramount for decision-makers in the above-mentioned jurisdictions, leading to protectionist and assertive approaches to digital governance. This resurgence of protectionism is evident in restrictions on semiconductor trade and discussions on international data transfers, cloud computing resources, and open-source software. This is best illustrated by the fact that Western countries, led by the United States, have barred Chinese 5G providers like Huawei and ZTE due to concerns over data security and surveillance by China’s government.<sup>2</sup> Similarly, Nvidia’s AI chips have been barred from exports into China and other “adversaries” that the US and the collective West have compiled. These developments contribute to increased fragmentation, mistrust, and geopolitical competition, and underscore the growing assertiveness towards digital sovereignty, on national (e.g. China) and supranational basis (e.g. the EU).

In the light of these present developments, **the big question for Global South countries is how to themselves also balance (1) dispersing their sovereignties** in order to support and advance multilateral initiatives such as the GDC (which comes with a lot of promise to benefit the Global South) **with (2) envisioning and asserting greater national and supranational<sup>3</sup> digital sovereignty** as a means of managing potential risks, including risks to their political and national sovereignty as a result of losing digital sovereignty.

---

<sup>1</sup> Obviously, there are smaller AI/digital governance ecosystems that have also been in formation, such as the British, Canadian, and Australian governance ecosystems; etc.

<sup>2</sup> Many experts have questioned the basis for these restrictions as little, if any, concrete evidence of surveillance and/or data security compromises have been shown so far.

<sup>3</sup> The adoption of the Euro across the EU member states is one of the best examples of implementation of a major policy supranationally. Continuing with this example where monetary sovereignty has become supranational (aka pooled sovereignty), similarly, digital sovereignty could probably be equally articulated, with both national and supranational levels of implementation. For example, a supranational digital sovereignty across the African Union.

