CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

Cloud Governance Project
Macro Cases

Digital Sovereignty

Key Considerations

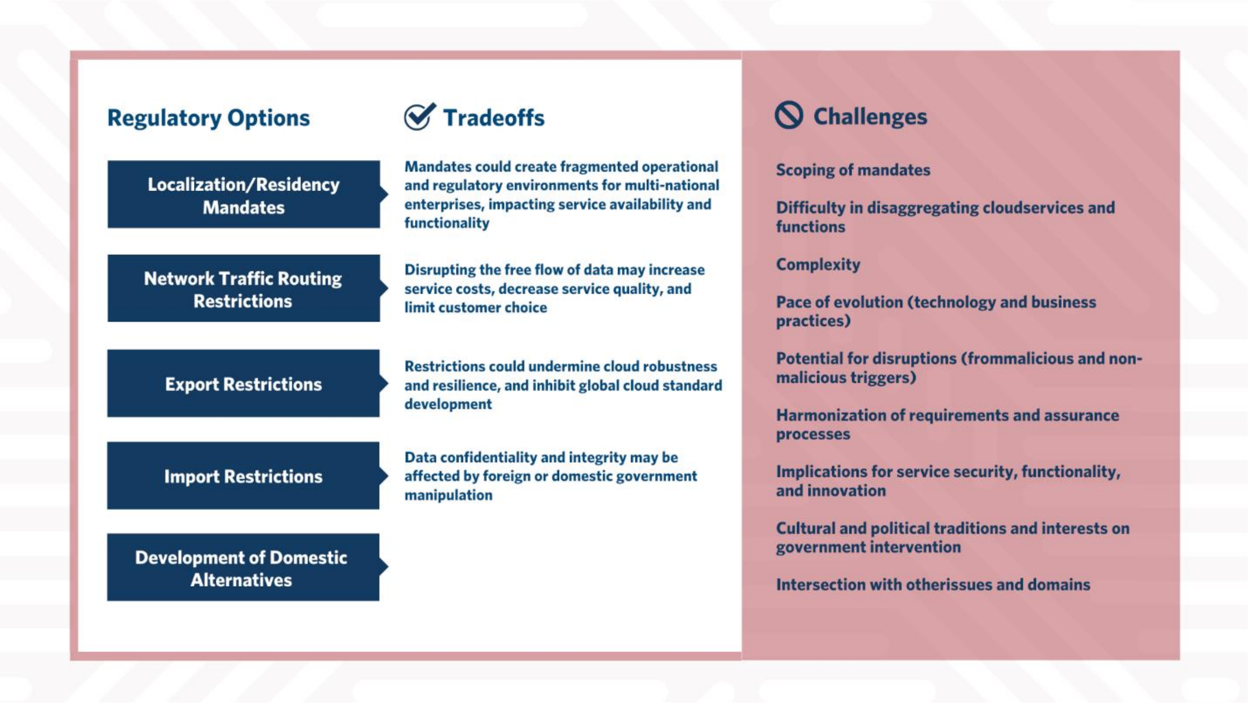
- ***Unwanted, potentially dangerous, precedent-setting.*** Digital sovereignty strategies may appear to enhance the privacy and security of cloud services, yet could also serve to legitimize restrictive practices by less-democratic regimes, stifle innovation, and degrade the quality of services that may be offered.
- ***Cloud system fragmentation.*** Differences in legal/regulatory environments and a lack of harmonization mechanisms may lead to different closed-off cloud environments in different countries/regions, contributing to the risk of a "fragmented" cloud.
- ***Different stakeholder perspectives.*** Incongruities in stakeholder values and priorities may complicate efforts to create a truly global policy environment for cloud services.
- ***Sensitivity of data.*** Forced transfer of sensitive data or intellectual property may be a prerequisite for foreign businesses to operate in a country or to make indigenous businesses competitive in national and global markets.

Background

As governments around the world seek greater control over the data, software, and hardware on which they and their populations rely, the term "digital sovereignty" has come to describe their general goal to assert control over information within their jurisdictions. While its precise definition is contested, "digital sovereignty" captures many governments' sense that they have ceded too much power over the internet and emerging technologies to foreign-based entities. Many argue that reasserting control will increase security, economic competitiveness, and protections for individual users.[1] Potentially neglected, however, are the trade-offs associated with applying this concept to cloud services, technologies that are owned and operated by private sector companies and derive much of their value proposition from economies of scale, the unhindered flow of data across borders, and transnational redundancy of data centers and digital infrastructure. Many of the regulatory options at policymakers' disposal to exercise sovereignty—from routing requirements to data localization mandates[2]—may threaten these features and erode the viability of the cloud as a global operating environment. Understanding the trade-offs and drawbacks of these approaches will be critical to policymakers' capacity to preserve the benefits of the cloud while safeguarding their societies and economies. This case explores why policymakers might pursue digital sovereignty strategies, the challenges in applying these strategies to cloud services, and the trade-offs involved in doing so.

While its precise definition is contested, “digital sovereignty” captures many governments’ sense that they have ceded too much power over the internet and emerging technologies to foreign-based entities. Governments have pursued digital sovereignty for a host of reasons, among them discomfort with foreign hosting of sensitive data, distrust of foreign cloud and IT service providers, concerns about international competitiveness, reliance on transnational supply chains for critical functions or industries, desires to promote healthy domestic cloud markets, geopolitical or geoeconomics fears, and worries about privacy protection and foreign interference. Kenya’s 2018 data localization requirements, for example, were drafted on the heels of an electoral scandal involving the ruling Jubilee political party and Cambridge Analytica, the now-defunct data analytics firm infamous for its collection and abuse of Facebook user information during the 2016 U.S. presidential election. These justifications may arise from legitimate concerns but nonetheless serve as cover for other political or economic goals.

Too often overlooked, however, are the clear risks or negative side effects of the various policy approaches used to advance digital sovereignty. For example, digital sovereignty can potentially erode the free movement of information and data, which has been at the core of the cloud’s success and promise. By extension, there is risk that such an approach might decrease the quality of service while increasing service costs. As countries and jurisdictions pursue different strategies toward digital sovereignty, divergence in the regulatory environment may weaken the cloud’s interconnectedness. This fragmentation of the global digital ecosystem—already underway, by some accounts—may put a cap on the potential benefits of the cloud while making the pursuit of an integrated global policy environment for cloud services far more difficult and elusive. And while there are regional attempts to harmonize the cloud environment, such as Europe’s Gaia-x initiative, the potential for digital sovereignty to increase fragmentation elsewhere, as countries respond to each other’s data localization, import, or routing restrictions with reciprocal or escalatory approaches of their own, cannot go overlooked.



Regulatory Options

Tradeoffs

Challenges

Localization/Residency Mandates

Mandates could create fragmented operational and regulatory environments for multi-national enterprises, impacting service availability and functionality

Network Traffic Routing Restrictions

Disrupting the free flow of data may increase service costs, decrease service quality, and limit customer choice

Export Restrictions

Restrictions could undermine cloud robustness and resilience, and inhibit global cloud standard development

Import Restrictions

Data confidentiality and integrity may be affected by foreign or domestic government manipulation

Development of Domestic Alternatives

Scoping of mandates

Difficulty in disaggregating cloudservices and functions

Complexity

Pace of evolution (technology and business practices)

Potential for disruptions (frommalicious and non-malicious triggers)

Harmonization of requirements and assurance processes

Implications for service security, functionality, and innovation

Cultural and political traditions and interests on government intervention

Intersection with otherissues and domains

Moreover, digital sovereignty is related not only to security and privacy, but also to national economic competitiveness. While governments in Europe, Asia, and elsewhere have been quick to identify competitiveness as a key reason to pursue digital sovereignty, they have paid far less attention to the potential for digital sovereignty to undercut competitiveness. For example, restrictions on cross-border data flows—which are oftentimes used to boost the competitive viability of domestic firms—erect economic and legal barriers for foreign enterprises while simultaneously undercutting the ability of domestic firms to serve international clients. This is especially true for small and medium-sized enterprises (SMEs) that lack the resources needed to navigate the increasingly complex patchwork of international data localization requirements. Unsurprisingly, these policies can deter SMEs from expanding into global markets, thus inhibiting access to foreign goods and services. As the cloud becomes more central to business success and prosperity, efforts to restrict, fragment, or weaken global cloud services may have knock-on consequences for innovation, economic performance, and commercial dynamism. Thus, there is a risk in governments being too heavy-handed in the pursuit of digital sovereignty.

Notes

[1] Julia Pohle and Thorsten Thiel, “Digital Sovereignty,” *Internet Policy Review* 9, Issue 4 (December 2021).

[2] See our analysis of the challenges associated with data localization and routing requirements: https://cloud.carnegieendowment.org/cloud-governance-issues/localization-and-routing-requirements/