Navigating Digital Sovereignty and its Impact on the Internet

December 2022

Executive Summary

Early this year, a broad alliance of citizens in Brazil published a Digital Sovereignty Charter[1]. In it, they lamented the rampant extraction and manipulation of local data by large technology companies and urged the government to support interoperable and open technologies, and data centers for common use.

Halfway around the world, in another vast and populous country, the government of India has instructed all service providers to retain information about their users for five years, and to synchronize their systems' clocks with only one source of time: the government's own servers. These are provisions in the new Indian Computer Emergency Response Team (CERT-In) cybersecurity directions[2] — a bid to increase security incident reporting and protect the country's digital infrastructure.

Both pronouncements project a vision of sovereignty in cyberspace, but the way they want to get to that vision, and the actors driving it, could not be more different.

The Internet Society began this study with the intent of developing a position on digital sovereignty. Far from a monolithic ideal, what we found was a broad and ill-defined notion that different groups interpret and apply diversely across the world. These include governments that wish to control how Internet operations and resources are run; local businesses that decry the dominance of foreign tech platforms; indigenous communities that want to safeguard local knowledge and resources; and individuals who want to assert their autonomy over their interactions with devices, platforms, and how they manage their data.

This report seeks to understand the different approaches that exist, recognizing that each one will impact the Internet differently, and to propose a framework for analyzing these effects. To

1 "Programa de Emergência para a soberania digital." https://cartasoberaniadigital.lablivre.wiki.br/carta/

2 CERT-In Government of India Ministry of Electronics and Information Technology (MeitY) Indian Computer Emergency Response Team (CERT-In), 2022. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

this end, it does not seek to solidify, or endorse, any single definition of, or position on, digital sovereignty.

This study narrows its scope to examine government-driven policies that have the explicitly co-opted digital sovereignty. It groups them according to their stated aims and assesses their impact on the technical foundation of the Internet. Our goal is to provide a nuanced guide to determining whether digital sovereignty policies may move us from an Internet that benefits everyone toward a series of fragmented, closed-off networks where the opportunities that arise from global connection are lost.[3]

It first presents a summary of policy trends in Asia-Pacific, Africa, and Europe — including Russia — then groups policies and measures based on (a) their objectives, and (b) the actors empowered to achieve their goals. This categorization highlighted two distinct approaches to digital sovereignty:

1. Policies that assert **national security through greater state control** intend to enforce laws in the digital sphere to bolster national security. This approach relies on empowered state actors to centralize control of network operations, concentrate power in the state, and limit the authority of operators. This type of digital sovereignty poses significant risks to the Internet's core values and characteristics and could lead to its direct fragmentation.
2. Policies that seek **economic self-determination driven by economic actors** want to strengthen actors in the national economy and, to a lesser extent, ensure supply chain resilience. These measures do not intentionally interfere with network operations of the Internet. Instead, they try to boost local digital economies by enabling a level playing field, and lower barriers to entry by making data and other resources more accessible. Some of policies could be protectionist and may interfere with network operations. On the whole, they seek to increase the opportunities created by a global network and connected societies and economies and may improve conditions for local actors to take advantage of the Internet.

This report shows that digital sovereignty policies may adversely affect how the Internet works, and more importantly, our ability to make use of the Internet. To minimize the risk of disrupting the operations of this global resource on which our economies and societies increasingly

3 While we appreciate academic discourse on sovereignty as a political concept, this report focuses on the consequences of the practical implementation of this notion on the Internet — specifically, how state-driven digital policies are impacting the technical foundation and evolution of the Internet.

depend, we strongly encourage policymakers to conduct an Internet Impact Assessment as part of their policy development processes, especially for measures that seek to address challenges in the digital environment.

Our initial analysis focuses on three regions, but acknowledges that digital sovereignty, whether implied or explicitly declared, is gaining traction in policy agendas across the world. Further studies on this issue may benefit from using this framework, and the Internet Way of Networking toolkit, to assess the effect that digital sovereignty policies may have on the global Internet, regardless of where these turn up.

Table of Contents

I. Introduction: What Is Digital Sovereignty?

The notion of "digital sovereignty" is historically associated with attempts by non-democratic governments to patrol Internet operations and resources within their borders. [4] In international policy discussions, the concept has been used to challenge existing Internet governance approaches that rely on decentralized and multi-stakeholder processes[5].

> Today "digital sovereignty" is being used more widely in varying contexts across the world, and to different ends.

It can include policy interventions to give individuals and groups more control over information, but also measures that give justice and interior ministries direct control over day-to-day Internet traffic. Many of these policies cover different facets of the digital domain — this study focuses only on those that may impact the operation of the Internet.

Policy interventions that fall under the umbrella of digital sovereignty may affect the Internet, but the term itself tells us little about what the impact is. Due to this ambiguity, the Internet Society does not take a position on digital sovereignty as a concept — the goal of this report is to assess how the varying policies that enact it may interact with the Internet.

1.1 The Concept of Sovereignty as We Know It

Visions of digital sovereignty vary significantly, due to differing interpretations of the concept of sovereignty itself. Sovereignty invokes ideas of authority and control, both at the individual and state levels, and these ideas are strongly colored by history, culture, and context. One aspect of sovereignty is the state's ability to exert power and control over resources and people in a given territory. In discussions of digital sovereignty, this extends to the ability of states to ensure their laws are obeyed in the digital realm and to limit the influence of external actors,

4 Adam Segal, "China's Alternative Cyber Governance Regime," Council off Foreign Relations, 13 March 2020 https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf

5 Julien Nocetti. "Contest and conquest: Russia and global internet governance." International Affairs 91.1 (2015): 111-130. Milton L Mueller., 'China and Global Internet Governance: A Tiger by the Tail', in Ronald Deibert and others (eds), Access Contested: Security, Identity, and Resistance in Asian Cyberspace (Cambridge, MA, 2011; online edn, MIT Press Scholarship Online, 22 August 2013)

including market dominance by foreign firms and their influence on domestic issues.

Sovereignty can also be understood in relation to other states, as a matter of independence from external pressure or influence, and in the national context as an assertion of political legitimacy and the rule of law. The recognition of a state's sovereignty by other states forms the basis of international law, and related treaties and agreements. In the digital sovereignty context, this externally focused perspective can translate to concerns of self-determination and the legitimacy of non-state actors' involvement in processes of governance.

Finally, sovereignty is also invoked to express the ability of individuals, and culturally distinct communities, to act with a reasonable degree of autonomy and make decisions independently. This view implies that the legitimacy to govern comes from consent of the governed, and in consequence, the individual's or a group's right to self-determination. As a result, some questions of digital sovereignty focus on the citizen's rights to privacy and freedom of expression in the digital space, particularly in relation to control of their data. ("Self-sovereign identity", or decentralized, non-platform dependent ways for individuals to assert their personal identification across the web, are not covered in this report.)

To add to these interpretations, digital sovereignty is often used in both overlapping and interchangeable ways with similar expressions: "technological sovereignty", "information sovereignty", "cyber sovereignty", "internet sovereignty", and "data sovereignty".

The term was first popularized in statements by the government of the People's Republic of China almost twenty years ago.[6] More recently, it has been used by people in the Global South to articulate a response to growing consolidation and corporate power on the Internet; in this context, digital sovereignty is a way to counter the "digital colonialism"[7] of the Global North.

1.2 Purpose of This Report

This report aims not to provide a definitive description of digital sovereignty, nor to investigate the nuances of its use in political discourse, but to accept that these variations exist and analyze

6 Ministry of Foreign Affairs of the People's Republic of China, "Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference," 16 December 2015, https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.

6 China.org.cn, "Full Text: International Strategy of Cooperation on Cyberspace," 7 March 2017, http://www.china.org.cn/chinese/2017-03/07/content_40424606_2.htm.

7 Julia Pohle and Thorstein Thiel. "Digital sovereignty". Internet Policy Review, 5 December 2020. https://doi.org/10.14763/2020.4.1532]

how the different interpretations of digital sovereignty can have very different impacts on the technical foundation of the Internet.

First, it summarizes recent trends in Asia-Pacific, Africa, and Europe (including Russia) — the regions where digital sovereignty has manifested most explicitly in public policy and government rhetoric. It then describes our methodology for analyzing relevant policy measures, and the main policy types we observed. We assessed these types using the Internet Society's **Internet Impact Assessment Toolkit**[8] and insights from regional trends, to determine the varying impacts of different digital sovereignty policies on the **Internet Way of Networking**[9] and key enabling characteristics of the open, globally connected, secure, and trustworthy Internet.

II. Regional Trends in Digital Sovereignty

This report sampled government policies in three regions that have overtly championed digital sovereignty.[10]

> There is no single narrative that describes digital sovereignty policies within regions or globally.

This reflects the different understandings and uses of the term, and the many and sometimes competing aims of policies introduced to further digital sovereignty.

We selected for our analysis national laws, policy proposals, strategy documents, and other public policy-related evidence that[11] either explicitly mentioned digital sovereignty, or a variation of it, in the policy text, or were introduced or publicized in a way that highlighted the term. While we found many policies around the world that may be pursuing digital sovereignty, this report excludes policies that did not clearly state it as an objective. This mitigates the risk of falsely attributing digital sovereignty to a policy that may have other motives.

8 The Internet Society, 'Internet Impact Assessment Toolkit', https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

9 The Internet Society, 'The Internet Way of Networking; Championing a Thriving Internet for Everyone', https://www.internetsociety.org/action-plan/2022/internet-way-of-networking/

10 While public discourse on digital sovereignty is shaped by multiple stakeholders, including academia and civil society, this report focuses on policies that governments themselves have introduced. with the explicit intention and proclamation of furthering their sovereignty over a multitude of aspects concerning the Internet

11 For brevity, we use the term 'policies' to encompass all of these measures and communications.

Government pronouncements and legal provisions were taken at face value—that is, we analyzed them based on their stated goals. More detailed information about policies and proposals in each region is set out in Appendix I.

2.1 Asia-Pacific

The main drivers of digital sovereignty measures in the countries we covered — Australia, China, India, and Viet Nam — are to protect national security, citizens, and social stability; and economic protectionism to bolster domestic industry. Other motivations include safeguarding social and cultural norms and values (as defined by the state) and helping people control their data.

China is a regional and global first-mover in defining, implementing, and exporting a state-centered approach to digital sovereignty, characterized by greater state control of the Internet and data localization. Other governments — for instance, Viet Nam — appear to be attracted to this model, and to the opportunities for greater investment in state capacity and the economy offered by China's Belt and Road Initiative.

China was one of the first countries to articulate the concept of digital sovereignty. In 2015, China's President, Xi Jinping, defined digital sovereignty as the right of each nation state to choose its own path of cyber-development and its own model of regulation and Internet policies, without interference from other countries.[12] Unusually, China's Data Security Law (2021) which aims to safeguard the "sovereignty, security and development interests of the state", asserts extraterritorial reach, assigning legal liability to entities that violate China's laws and interests in the course of processing data abroad.[13]

China has also operationalized digital sovereignty through data localization regimes. Its Internet Domain Name Regulations 2017[14] support the growing trend toward localization; specifically, rules that require root-server operators, and domain name registries and registrars, to be based in the country.[15]

12 Ministry of Foreign Affairs of the People's Republic of China, "Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference," 16 December 2015, https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.

13 The National People's Congress of the People's Republic of China, "Data Security Law of the People's Republic of China," 10 June 2021, http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml.

14 China Internet Network Information Center, "Internet Domain Name Regulations," 26 October 2017, https://www.cnnic.com.cn/PublicS/fwzxxgzcfg/201710/t20171026_69608.htm.

15 Rogier Creemers, "China's Approach to Cyber Sovereignty," Konrad-Adenauer-Stiftung, 2020, https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537.

State control is also seen as a way of boosting the domestic digital economy and providing preferential treatment to Chinese companies.[16]

Australia's Cyber Security Strategy 2020 aims to spur "new sovereign Australian cyber capabilities and companies" and "promote innovation in sovereign cyber security research and[17] development,"[18] yet the overall picture is an effort to balance national security interests with a liberalized trade agenda. Australia has yet to require data localization: Its national hosting strategy does not prescribe domestic ownership and control or localization of government data and was recently changed so that non-Australian-owned and based companies may qualify.[19]

India wants to increase state power and access to data, but considers economic, rather than purely security interests. Its draft data localization law has recently been shelved, and the government's approach is broadly framed as protecting critical infrastructure and data in the wake of data breaches, and bolstering hosting capacity and the digital economy.

2.2 Africa

The concept of digital sovereignty in Africa is relatively recent, gaining prominence and usage in the last five year.

> Discourse on digital sovereignty is shaped by Africa's colonial history, in the context of the ongoing unequal distribution of wealth and power.

Many African countries' digital spaces remain largely dependent on foreign firms — mostly from the West, but more recently also from China — and African countries have little control of the data and the infrastructure they depend on, and are not economically benefiting as expected.[20]

---

16 Jane Li, "Beijing has a new legal architecture for sweeping control over user data," Quartz, 30 August 2021, https://qz.com/2051268/china-aims-to-control-but-also-unleash-the-economic-power-of-data/; and Rogier Creemers, "China's Approach to Cyber Sovereignty," Konrad-Adenauer-Stiftung, 2020, https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537.

17 Australia is considering a data localization regime. See Justin Hendry. "Tech giants rally against data localisation in Australia," InnovationAus.com, 7 September 2022. https://www.innovationaus.com/tech-giants-rally-against-data-localisation-in-australia/

18 Australian Government, "Australia's Cyber Security Strategy 2020," https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

19 Joseph Brookes, "Certified Strategic data centres double," InnovationAus.com, 20 August 2021, https://www.innovationaus.com/certified-strategic-data-centres-double/.

20 David Monyae, Centre for Africa-China Studies at the University of Johannesburg, 'Africa's digital sovereignty a timely and relevant debate', September 28, 2021 https://www.uj.ac.za/news/africas-digital-sovereignty-a-timely-and-relevant-debate/

Digital sovereignty, as used by African governments, is typically framed as an extension of national sovereignty, and has firm roots in the political conception of sovereignty promoted by China.[21] There are relatively few policy and regulatory frameworks or decisions on digital sovereignty in the region's fifty-four countries, and so far, the idea tends to be articulated through political statements. The policies that do, such as the African Union's Digital Transformation Strategy for Africa, South Africa's draft Data and Cloud policy[22], and Rwanda's Data Revolution Policy"[23], stress economic self-determination by ensuring local ownership and control over locally generated data.

There is a growing trend to replicate the Chinese data governance model which requires all servers to be located within a country's borders, providing the state with easier access to information. Governments in Nigeria and Senegal increasingly connect digital sovereignty with protecting or increasing the role of the state. Governments are also looking to address their own concerns about political control and economic benefits of the Internet flowing out of their countries.

2.3 Europe, Including Russia

The European region is home to the European Union (EU) and the Russian Federation, two leading powers with distinctive visions for the future of the Internet. The countries or entities analyzed exert international influence and have articulated and implemented a vision of digital sovereignty. Two main camps were identified in the region.

The first camp — the EU and its member states, France, Germany, and Italy — frame digital sovereignty primarily in the context of economic competitiveness, developing local industry, and protecting against cyberattacks.

> Economic sovereignty can mean reducing supply chain dependencies so key infrastructure is not overly reliant on foreign providers, and encouraging the development of alternatives to currently dominant, non-European firms.

21 Monyae, 2021

21 African Union, "The Digital Transformation Strategy for Africa (2020-2030)"

22 Government of South Africa, Department of Communications and Digital Technologies, 'Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy', https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

23 "Rwanda National Data revolution and Big data", 2017 http://statistics.gov.rw/publication/rwanda-national-data-revolution-and-big-data

To a lesser extent, some policies seek to empower an individual's sovereignty over their data. The Digital Services Act[24] and European Data Act[25] aim to give businesses and individuals more choice of service and control over user-generated data, backed by regulatory action.

While these framings tend to be initiated by governments, they do not exclusively place state authority at the center. Their enacting policies involve increased roles for regulators but have a stated aim to empower businesses or individuals.

The second camp in this region — with the Russian Federation as the strongest example — equates digital sovereignty with greater state control over the digital realm and the information that passes through it, specifically data flowing within the country.

The Russian Federation does not commonly refer to 'digital sovereignty' in policy documents but does so in government press releases and public statements. A 2019 regulation informally called the "Sovereign Internet Law" aims to ensure continued Internet connectivity in the face of an attack on infrastructure by foreign actors.[26]

III. Objectives and Outcomes: Approaches to Digital Sovereignty

The policies and measures covered in this report are explicitly driven by digital sovereignty, but they vary in the officially stated objectives and may enable different, at times non-state, actors to achieve its goals.

3.1 Four Main Policy Objectives

1. **National security and the ability to enforce laws:** These policies address threats to **national security**, specifically foreign cyber-attacks, and online vulnerabilities. Through them, the state aims to secure the digital domain within its borders. These can cover cyber-security of critical infrastructure all the way to the use of Internet technologies in political processes and change. Many governments have encountered friction in exerting authority over digital assets and services operating or made available locally and want to reassert their **ability to set and enforce laws**

24 European Commission, 'The Digital Services Act: ensuring a safe and accountable online environment', https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

25 European Commission, "Data Act," https://digital-strategy.ec.europa.eu/en/policies/data-act

26 'Федеральный закон от 01.05.2019 № 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации"', http://publication.pravo.gov.ru/Document/View/0001201905010025

within their territory. This typically characterizes policies that enable lawful access to information by law enforcement agencies, competition authorities, and other regulators. Beyond controlling locally generated data, this authority can extend to how services and software operate in a specific national context.

2. **Economic self-determination**: These policies strengthen local industry development by creating more opportunity for national companies to compete, often in an environment seen to be dominated by technology companies from the United States and, increasingly, in some countries, China.[27] Some of the policies attempt to meet this objective through strong protectionist measures, while others foster market forces to create a more level playing field.
3. **Protecting rights and empowering citizens/users and communities:** These policies bolster individual and collective autonomy vis-a-vis the technology platforms they interact with, specifically by giving citizens and communities the ability to take action and make decisions relating to their data and digital activities.
4. **Upholding societal norms and value:** These policies preserve local norms and traditions, or those which a government wishes to encourage, amidst the influx of technologies, standards and services that are seen to embody or promote other social, cultural, and political values. This is often secondary to others, i.e., it is rarely the dominant objective.

Policies often have several overlapping goals: a data localization policy may affirm citizens' rights over their data while also preventing that data from being stored abroad for security reasons. Policies may also have implicit goals; data localization may likewise enable intelligence actors and law enforcement agencies to more readily access citizens' data, or to generate business for local data centers.

3.2 Actors Empowered to Achieve Policy Objectives

Policies with similar goals may affect the Internet differently, depending on who is empowered to achieve them. This may be (1) the state, by increasing the authority of its institutions; (2) economic actors, by fostering a fair and competitive environment for businesses; and/or (3) citizens, both by expanding their rights and entitlements, with regulatory backing to assert their will.

These goals and empowered actors are not exhaustive, having been drawn from policies sampled in only three regions. We recognize that policies on digital sovereignty are emerging

27 Julia Pohle & Thorstein Thiel. Digital sovereignty. Internet Policy Review, 9(4), 5 December 2020. https://doi.org/10.14763/2020.4.1532]

across the world, and propose that the analytical framework presented here may apply to other policies on this issue, in the regions we studied, and in others.

IV. Common Approaches to Digital Sovereignty and Their Impact on the Internet

Most countries have a mix of policy objectives and empowered entities, but having assessed 34 policies, two distinct digital sovereignty approaches emerged above others:

(1) **National security driven by increased state control** and
(2) **Economic self-determination driven by economic actors**

Several policies aimed to increase individual and/or community sovereignty primarily by giving citizens and/or cultural groups more control over their personal data, but there were not enough examples of these being implemented to merit a third distinction. For more information about the methodology and the policies included in the analysis, see Appendix III & IV.

To analyze if and how digital sovereignty affects the Internet, we use the Internet Impact Assessment Toolkit (IIAT)[28] a framework that describes the conditions that the Internet needs to exist and thrive as a public good. We evaluate each policy type against each critical property of the Internet's 'Way of Networking'[29] and the enablers[30] that underpin an Internet that is open, globally connected, secure, and trustworthy. Both are articulated in greater detail in Appendix II.

Factors such as the political system, rule of law, prior technical implementations, or protection of civil liberties can all shape the effect of a policy but are not part of this analysis.

4.1 Approach 1: National security driven by increased state control

Objective: National security and, to a lesser extent, the ability to enforce laws in the digital sphere
Empowered Entity: The state
Relevant jurisdictions: Australia, China, Nigeria, Russia, Viet Nam

28 The Internet Society, "Internet Impact Assessment Toolkit", https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

29 The Internet Society, 'The Internet Way of Networking', 'Critical Properties', https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/

30 The Internet Society, 'Enablers of an Open, Globally Connected, Secure and Trustworthy Internet', https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/

This approach is characterized by policies on national security that seek to reinforce the state's authority within its territory and its ability to enforce its laws in the digital domain. It strongly emphasizes the role of the state in implementation, and invariably increases the power, and often capacity, of the state to impact the Internet.[31]

Impact on the Internet Way of Networking

Centralization of control over infrastructures is the most common and concerning impact on the Internet of national security policies. These typically seek to have the state control key networking infrastructures, such as naming and addressing, that are decentralized and distributed on the Internet. The policies often strengthen the authority of the state to direct network operations, and in some cases even to manage them.

A prominent example is Russia's "Rules for the centralized management of a public communication network", part of the legislation known as the "Sovereign Internet Law" which aims to impose greater control over traffic flows within the country. In delegating authority to the federal agency Roskomnadzor, it mandates that intermediary servers be installed to filter and monitor traffic on Russian networks. This directly interferes with the ability of Russian network operators to manage their own networks, obliging them to conform to Roskomnadzor's routing policy requirements.

Similar provisions are found in Viet Nam's "Law on Cybersecurity", which delegates significant power to the Cybersecurity Authority to restrict and suspend network operations, including filtering information deemed to disrupt security or disturb public order.

Centralization extends to other technical functions. India's "CERT-In cybersecurity directions" expand state control to setting network time-coordination, by requiring all entities and servers to connect to the government's Network Time Protocol (NTP) servers.[32] These laws interfere with the distributed operation of both routing (via the Border Gateway Protocol, or BGP) and name resolution (using the Domain Name System, or DNS).

Some policies **restrict the voluntary deployment of certain infrastructure technologies and protocols**, which can severely affect interoperability. For instance, both China's "Cybersecurity

31 Several policies stated a desire to limit disinformation and misinformation to foster a more cohesive society. These have at times been construed as efforts to control the flow of information within a nation's borders. This report refrains from adopting these interpretations to avoid assumption, focusing strictly on the policies' stated aims.

32 The Internet Society, 'Internet Impact Brief: India CERT-In Cybersecurity Directions 2022', https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-india-cert-in-cybersecurity-directions-2022/

Law" and Viet Nam's "Law on Cybersecurity" require Internet intermediaries to monitor content. This prevents intermediaries from using community-developed and widely adopted security building blocks (for example, Transport Layer Security, or TLS 1.3) and other best practices that rely on encryption. To track or scan for content, infrastructure intermediaries may need to specialize and adapt their services to accommodate specific types of content, causing **significant harm to the technology-neutral and general-purpose nature of the Internet**.

Digital sovereignty policies on national security often directly disrupt Internet operations. They pose significant risks to the global Internet by inducing a fragmentation of the network through **interference with the Internet's shared set of identifiers**. For instance, supporting documentation to Russia's Sovereign Internet Law mandates the use of government-controlled DNS resolvers. Requiring Russian operators to use only these DNS resolvers will enable the government to unilaterally modify name resolution in Russia[33], potentially creating a Russian alternative to the global DNS.

In summary, digital sovereignty policies on national security can have severe impacts on the Internet's networking model and do significant harm to this open and globally connected platform.

Impact on the Open, Globally Connected, Secure, and Trustworthy Internet

In addition to impairing the attributes that make the Internet work properly, these policies can also affect the broader enablers of an open, globally connected, secure, and trustworthy Internet. One of the clearest casualties is the **trustworthiness** of the Internet, which lessens with interference on basic functions like naming and addressing. If the unilateral increase in state control is not matched by transparency in decision-making, it can also degrade **accountability** in the online environment. While laws may be supplemented by more detailed documentation on accountability measures, we have not been able to locate any in the policies we studied.

A common thread across all policies of this nature is the breadth of vaguely defined activities that fall under expanded state authority, with few checks or conditions on how these powers are exercised. India's revised CERT-In Cybersecurity Directions[34] transforms the role of CERT-In from an authoritative entity in a system of voluntary collaboration and information-sharing, to a quasi-regulator or even a law enforcement agency.

33 Принят закон о «суверенном интернете»', http://duma.gov.ru/news/44551/

34 CERT-In Government of India Ministry of Electronics and Information Technology (MeitY) Indian Computer Emergency Response Team (CERT-In), 2022. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

Filtering and monitoring techniques reduce the **confidentiality and integrity of information.** This is exemplified by Russia imposing interception equipment to scan and filter content[35] These, along with extremely broad data retention requirements in India and personal data verification in Viet Nam severely threaten users' privacy. China's requirement that services obtain consent when collecting personal information could enhance user **privacy but** is strongly outweighed by obligations to conduct mass surveillance and report users' "unacceptable behavior," and their transmission of "prohibited information".

Centralized control over key functions, and applying technical means to intercept and monitor traffic, also diminish the **resilience, availability, and reliability** of networked services. India's time security (NTP) proposal risks creating a single point of failure that is detrimental to all services in the country, including the encryption technologies that depend on this function. Russia's use of network eavesdropping equipment can cause significant outages to the broader network if those devices and their associated software malfunction. In fact, there have already been reports of such outages,[36] and the law itself recognizes this risk by allowing the equipment to be bypassed should it fail to work properly.

The policies analyzed are overall detrimental to an open and globally connected Internet. **Collaboration** among stakeholders, which has been the norm in Internet governance and operation, is supplanted by centralized state control, undermining important benefits offered by the networking model. Policies to restrict and direct **reachability** on the network, including by interfering with DNS and routing decisions, limit the resources available to users to only those permitted by the government. There are also indirect consequences; new operational requirements and increased compliance costs raise barriers for network operators and intermediaries, ultimately limiting the Internet's **ease of access**.

4.2 Approach 2: Economic Self-determination Driven by Economic Actors

Objective: Economic self-determination, i.e., strengthening actors in the national economy, and ensuring supply-chain resilience
Empowered Entity: Economic actors, typically firms
Relevant jurisdictions: EU, India, Rwanda, South Africa

35 A Ten Minute Introduction to Middleboxes http://yuba.stanford.edu/~huangty/sigcomm15_preview/mbpreview.pdf

36 '«Суверенный интернет» засбоил. Проблемы с оборудованием привели к системным сбоям', 2021, https://kapital-rus.ru/articles/article/suverennyi_internet_zasboil_problemy_s_oborudovaniem_priveli_k_sistemnym_sb/

This approach is characterized by policies that assert economic self-determination by strengthening the national economy. It aims to reduce the dominance of and reliance on foreign technology and service providers by (1) creating more opportunities for local companies to compete, at times with a degree of protectionism, and (2) cultivating supply chain resilience for the local digital sector. While these policies often sought to extend state authority, for example, by growing competition regulators' remit, they also sought to empower actors in the broader economy.

Impact on the Internet Way of Networking

The economically driven policies we analyzed do not directly interfere with network operations of the Internet. Aware of the opportunities created by a global network and connected societies, these policies more often focus on improving the conditions that allow local actors to take advantage of the Internet.

In many cases, these explicitly aim to strengthen important features of the networking model. For instance, the African Union's "Africa Digital Transformation Strategy (2020-2030)" promotes technology-neutral approaches for cross-border interoperability. India's Data Centre Policy similarly urges voluntary adoption of established global standards.

At face value, the policies analyzed uphold the open and global Internet as an asset to be supported and harnessed for regional and national economic progress.

Impact on the Open, Globally Connected, Secure and Trustworthy Internet

Digital sovereignty policies on economic self-determination largely support the enablers of an open, globally connected, secure, and trustworthy Internet. **Access and lowered barriers to entry** are viewed as key to the Internet becoming a source of opportunity. The African Union's "Africa Digital Transformation Strategy (2020 – 2030)" seeks to make devices and services more affordable, stressing governments' role in developing infrastructure to expand access and **capacity**. This includes Internet Exchange Points (IXPs) to improve interconnection and traffic exchange, and a regulatory environment that proactively supports access solutions such as community networks.[37] Beyond deploying infrastructure, the EU's Data Act seeks to lower "legal, economic, and technical" barriers to data access, notably by requiring providers to have technical tools for users to control how their data is shared with third parties. The European

37 Internet Society Action Plan 2022, last modified 6 September 2022. https://www.internetsociety.org/action-plan/2022/community-networks/

Commission claims that making more data available for reuse will add €270 billion to the region's GDP by 2028.[38]

However, these policies may also constrain flexibility in **technical deployment**. For instance, the Indian Data Centre Policy favors indigenous hardware and software to reduce the country's overall imports. Strict enforcement may limit the use of potentially more cost-effective and suitable, but non-Indian, technologies. Similarly, the EU Data Act's specific standards mandate, intended to encourage greater interoperability, may hinder businesses from developing innovative technologies.

Nevertheless, these policies recognize that choice and availability of technology are integral to a **reliable and resilient** digital environment.

> From India promoting reliable electricity supply to data centers, to the EU shoring up digital components supply, and the African Union backing routing security to enhance digital security — many policies foster supply-chain resilience as a key aspect of economic digital sovereignty.

Unlike national security policies, these economically focused measures uphold the **confidentiality and integrity** of information, for instance by bolstering strong encryption. In the African Union's Digital Transformation Strategy, this emphasis went in tandem with strengthening user control of personal data and other improvements to **privacy**.

4.3 Other Approaches to Digital Sovereignty

A third approach aligns digital sovereignty with individual and/or collective sovereignty. This is manifested in measures to enhance the rights of individuals and/or communities in relation to data about or created by them. In its data sovereignty guidance[39], the New Zealand government calls for institutions to choose cloud services that respect indigenous Māori data rights. It upholds the Māori Data Sovereignty Charter,[40] which urges greater Māori access to, and

38 "Data Act: Commission proposes measures for a fair and innovative data economy," 23 February 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

39 New Zealand Digital Government. "Data Sovereignty." https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/help/data-sovereignty/

40 "Maori Data Sovereignty Charter." https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/5913020d15cf7dde1df34482/1494417935052/Te+Mana+Raraunga+Charter+%28Final+%26+Approved%29.pdf

ownership of, data collected about them by other entities, and empowers the Māori to govern their data according to their customs and priorities.[41]

In a parallel vein, the EU Data Act makes data available across different sectors of the economy by giving data owners — both individuals and businesses — more control over how their data is shared with third parties. This is very close to the concept of "individual sovereignty", with authority decentralized and delegated to the entities that own the data, in line with the subsidiarity principle of making decisions as close as possible to where their impact is felt.

This approach departs from the classic, state-centered, and territory-based concept of sovereignty[42], moving towards equipping individuals with the means to act and decide in a conscious, deliberate, and independent manner.

By doing this, the Data Act facilitates the availability, portability, and use of data, but building barriers to entry for non-EU technology. By clarifying the roles and responsibilities of entities in the value chain, it simplifies accountability, reinforcing the Internet's trustworthiness. But the Data Act also contains provisions more commonly associated with traditional state sovereignty, such as international data transfer restrictions or potential interoperability and specific standards mandates. These may negatively impact not only the Internet enablers but also the Internet Way of Networking.[43]

Finally, a fourth policy approach focuses on safeguarding cultural norms and values. This objective was frequently combined with others, such as national security or economic self-determination, and did not feature prominently in digital sovereignty policies.

41 "Principles of Māori Data Sovereignty." October 2018. https://cdn.auckland.ac.nz/assets/psych/about/our-research/documents/TMR%2BM%C4%81ori%2BData%2BSovereignty%2BPrinciples%2BOct%2B2018.pdf

42 Julia Pohle and Thorstein Thiel. Digital sovereignty. Internet Policy Review, 5 December 2020. https://doi.org/10.14763/2020.4.1532]

43 Another policy often associated with increased control over personal data is the EU's General Data Protection Regulation (GDPR). While GDPR does indeed echo the sentiments of individual sovereignty, it was excluded from the scope of this paper due to the fact that the text of the regulation does not make reference to digital sovereignty as well as that the regulation predates the use of the term in EU strategy documents.

V. Conclusion

As a global network of networks, the Internet does not conform to the notion of national borders. Networks may operate in certain jurisdictions, yet their topology and interconnection points are defined by the goal of optimizing traffic, rather than following a political map. Interconnection rules are defined not by treaties but are based on well-functioning voluntary processes and collaboration among networks.

It is in this context that we find the notion of sovereignty, which predates the Internet, being increasingly applied to the digital realm. Digital sovereignty policies have a variety of goals: from keeping data within national borders to harnessing technology to drive indigenous development — and their effects on the Internet range from few or none, to potentially risky, to directly damaging, and fragmenting, the global Internet.

The concept of digital sovereignty itself remains vague and disjointed — hence the difficulty in generalizing its impact. To better understand its numerous facets, this report focused on how digital sovereignty is applied in public policy. By assessing dozens of state-issued policies in different countries in Asia-Pacific, Europe, and Africa, we identified how various government approaches to digital sovereignty can have a different effect on the Internet.

Policies that seek to bolster national security through increased state authority concentrate control in the government, and excessively limit the autonomy of networks. These measures risk damaging the Internet by enforcing specific technical requirements and relying on a "command and control" model, rather than on peer-to-peer collaboration and coordination. Some policies directly frustrate the critical properties that make the Internet work properly, such as its decentralized management and its use of global identifiers (naming and addressing). Efforts that fundamentally change the way the Internet works limits the value we can derive from the Internet as an open and globally connected resource.

Policies that pursue economic self-determination by empowering economic actors tend to focus on boosting local digital economies by leveling the playing field and lowering barriers to entry by making resources, such as data, more accessible. These policies tend to be better aligned with the way the Internet works as they are not at odds with its properties and enablers. However, some of the measures covered in this report have significant elements of protectionism, for example, limiting availability and choice in products and services. But overall, these policies may only cause minimal harm, and in some cases, may even enhance and reinforce the Internet's utility.

An emerging, less common approach, found in the EU Data Act and New Zealand's data sovereignty guidelines, evoke the sovereignty of the individual, and of distinct communities, specifically their ability to act and decide for themselves when it comes to their digital

presence. This orientation appears to be more aligned with how the Internet works, and the principles that underpin it: decentralized management of networks, unrestricted use of technologies, unrestricted reachability, and transparency and accountability in using Internet resources. Although examples of this approach are limited, it represents a user-centric vision of sovereignty in the digital world.

Typically, strategies for digital sovereignty have a mix of approaches, albeit one or two usually dominate. Distilling the dominant policy goals allowed us to assess the impact that a specific digital sovereignty approach may have on the foundation of the Internet.

Digital sovereignty is an expanding concept—and the notion alone tells us little about how it may reshape the online environment. Ultimately, it is the resulting policies and the actors they center and empower that define the impact of digital sovereignty on the Internet.

Like any live ecosystem, the Internet is constantly evolving. This continuing evolution without a centralized plan or authority underpins its value to the world. But as the Internet has come to permeate most of our lives, governments and businesses increasingly make decisions that impact it.

Each new policy proposed under the name of digital sovereignty needs to be assessed to ensure it does not damage the elements that make the Internet useful to us, nor move us closer to a series of fragmented, closed-off networks where the opportunities that arise from global connection are lost.

This report shows how that assessment can be done, both on the policies we examine here, and on those to come.

Appendix I — Regional Trends in Digital Sovereignty

A. Asia-Pacific

The Asia-Pacific region includes the world's most populous countries, China and India, and some of its smallest. The countries we examined are large economies with considerable geopolitical influence in the region, and globally. They have drafted or adopted one or more policies, laws, regulations, and/or strategies that refer to digital sovereignty or similar terms,[44] but exhibit great variety in interpreting and operationalizing digital sovereignty.

Australia – In Australia, digital sovereignty-driven policies focus on improving cybersecurity. Its Digital Government Strategy aims to protect and manage public information with "appropriate privacy, sovereignty and security controls"[45] and is supported by a Hosting Strategy that addresses "risks to the sovereignty of data held in Australian Government data centers".[46] Tangentially, these strategies encourage the building of domestic data centers.

Despite the absence of mandatory data localization requirements in Australia, recent official reports highlight unprecedented levels of foreign interference aimed at undermining Australia's national sovereignty.[47] In response, researchers have urged more digital sovereignty measures to safeguard both national security[48] and economic interests,[49] along with data localization requirements for government data.[50]

China – China, being one of the earliest adopters of the concept of digital sovereignty, has had the longest period of time to operationalize its vision. It exerts influence in defining a specific approach to digital sovereignty in the region and globally.

China's perspective has shaped many policies and laws in the country, although it is not always explicitly stated. The goal to uphold "cyber or Internet sovereignty" can be found in the

---

44 For example, Viet Nam frequently uses the term 'national sovereignty in cyber-space'.

45 Digital Transformation Agency, Australian Government, "Digital Government Strategy," 2021, https://www.dta.gov.au/sites/default/files/2021-12/Digital%20Government%20Strategy_web-ready_FA.pdf.

46 Digital Transformation Agency, Australian Government, "Whole-Of-Government Hosting Strategy: Overview," https://www.dta.gov.au/our-projects/hosting-strategy/overview.

47 Independent National Security Legislation Monitor, Australian Government, "Annual Report 2020-2021," 2021, https://www.inslm.gov.au/sites/default/files/2022-01/inslm-annual-report_2020-21.pdf.

48 Andrew Mitchell, "A sovereign Australian government data framework," Australian Strategic Policy Institute, 11 August 2021, https://www.aspistrategist.org.au/a-sovereign-australian-government-data-framework/

49 Marcus Thompson, "Australia's own assets can ensure national digital resilience," The Mandarin, 6 May 2022, https://www.themandarin.com.au/188379-australias-own-assets-can-ensure-national-digital-resilience/.

50 Andrew D. Mitchell and Theodore Samlidis, "Cloud services and government digital sovereignty in Australia and beyond," International Journal of Law and Information Technology, January 2022, https://www.researchgate.net/publication/358197261_Cloud_services_and_government_digital_sovereignty_in_Australia_and_beyond.

Cybersecurity Law (2017), Data Security Law (2021), and the International Strategy of Cooperation on Cyberspace (2017). Through such measures, and in high-level political narratives, China views digital sovereignty as a way to ensure national security, protect the country from cyber-threats,[51] and build the local digital economy by providing preferential treatment to Chinese companies.[52] [53]

Several laws affirm China's intent to take extra-territorial measures, such as blacklisting foreign companies that don't comply with its regulations. The Cybersecurity Law (2017) requires network operators in critical sectors to store within China any data they gather or produce in the country. Business information and data on Chinese citizens gathered within China must be kept on domestic servers and not transferred abroad without permission. These provisions are reinforced in the Personal Information Protection Law (2021).[54]

India – Relevant digital sovereignty measures in India, limited to data localization requirements and policies that explicitly refer to the term, are mostly in draft form. These policies prioritize critical infrastructure and data protection in the wake of data breaches and bolster the country's hosting capacity. Digital sovereignty is cited as a driver for India's draft Data Center Policy (2020)[55] which, alongside security goals, aims to decrease dependencies in the supply chain. It aligns itself with the recent "Atmanirbhar Bharat" initiative (loosely translated as an India which is self-dependent and self-sufficient), which aims to incentivize economic development.

Viet Nam – Digital sovereignty, translated as "national sovereignty in cyberspace", was adopted in Viet Nam's Law on Cybersecurity (2018). It emboldens the Ministry of Public Security to "prevent and combat the use of cyberspace to infringe national sovereignty, interests and security, social order and safety."[56] This includes tackling disinformation, and improving defense via detecting, countering and preventing attacks in cyberspace. The law requires foreign providers of online services to localize data storage, and to have an in-country office presence.

---

51 China.org.cn, "Full Text: International Strategy of Cooperation on Cyberspace," 7 March 2017, http://www.china.org.cn/chinese/2017-03/07/content_40424606_2.htm.

52 Jane Li, "Beijing has a new legal architecture for sweeping control over user data," Quartz, 30 August 2021, https://qz.com/2051268/china-aims-to-control-but-also-unleash-the-economic-power-of-data/; and Rogier Creemers, "China's Approach to Cyber Sovereignty," Konrad-Adenauer-Stiftung, 2020, https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537.

53 The National People's Congress of the People's Republic of China, "Data Security Law of the People's Republic of China," 10 June 2021, http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml.

54 Digi China, Stanford University, "Translation: Personal Information Protection Law of the People's Republic of China — Effective Nov. 1, 2021," 7 September 2021, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

55 MeitY, "Data Centre Policy 2020: Draft for Discussion," https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf.

56 Unofficial translation of Law on Cybersecurity, 12 June 2018, https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf.

Network services in data and content can be halted at the order of the authorities. The law does allude to increasing "self-autonomy" in cybersecurity and child protection, but defines the term vaguely, and does not specify how this will be safeguarded.

Elsewhere, Viet Nam's Strategy for National Protection in Cyberspace[57] refers to state-centric digital sovereignty. The concept also appears in political speeches.[58] It is applied by the Ministry of National Defense in Viet Nam's military context, situating it as central to defending against external threats. Viet Nam established a Cyber Command to "protect the national sovereignty in cyberspace".[59] In summary, with some moments of resistance to China's growing influence,[60] Viet Nam is consolidating its digital sovereignty framework and approach through a variety of laws and policies that draw on China's model.[61] [62]

B. Africa

African Union – In 2020, the African Union's Digital Transformation Strategy for Africa set out a ten-year economic strategy that includes ensuring Africa's ownership of digital tools by localizing infrastructure and data storage.[63] It intends to reduce the dominance of mostly US and European technology firms by building local infrastructure, funded by a digital sovereignty fund,[64] that is expected to reduce costs and latency in international connectivity, and increase local control over communications, ultimately allowing Africa to meet its own needs. It calls for an Africa Data Center Infrastructure to host mission-critical servers and systems and aspires to localize citizens' personal data.

South Africa – The draft Data and Cloud Policy[65] treats data as an asset to be protected, and exploited, by improving the country's data analytics capacity, and requiring all 'critical

57 Anh Kiet, "Vietnam tightens national sovereignty protection in cyberspace," Hanoi Times, 9 December 2021, https://hanoitimes.vn/vietnam-tightens-national-sovereignty-protection-in-cyberspace-319495.html.

58 Ibid.

59 Ministry of National Defence, Vietnam, "Cyber Command asked to safeguard national sovereignty in cyberspace," 1 September 2018, https://vietnamnews.vn/politics-laws/420790/cyber-command-asked-to-safeguard-national-sovereignty-in-cyberspace.html

60 Justin Sherman, "Vietnam's Internet Control: Following in China's Footsteps?" The Diplomat, 11 December 2019, https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/.

61 Justin Sherman, "Vietnam's Internet Control: Following in China's Footsteps?" The Diplomat, 11 December 2019, https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/.

62 Deborah Elms, "Digital Sovereignty: Protectionism or Autonomy?" Hinrich Foundation, September 2021, https://www.hinrichfoundation.com/research/wp/digital/digital-sovereignty-protectionism-or-autonomy/.

63 African Union,"The Digital Transformation Strategy for Africa (2020-2030)" https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

64 Create a harmonized environment necessary to guarantee investment and financing by setting up a digital sovereignty fund in order to close the digital infrastructure gap and achieve an accessible, affordable and secure broadband, across demography, gender, and geography, https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

65 David Monyae, 2021

information' to be stored and processed locally. It asserts ownership over all data generated in South Africa,[66] and approaches digital sovereignty as a means to economic development.

Rwanda – Rwanda's government was among the first to explicitly support digital sovereignty, asserting the country's ownership of all data generated within its borders. Its 2017 "Rwanda Data Revolution Policy"[67] aims to build a data-enabled industry and to localize data for security and privacy.

Nigeria – One measure, the Nigeria cloud computing policy of 2019,[68] explicitly invokes data sovereignty. It encourages public sector uptake of cloud services, and new requirements for the treatment of national data. Digital sovereignty has also featured prominently in political rhetoric, especially following the country's Twitter ban in 2021 - 2022[69]. Concerned that citizens were using Virtual Private Networks (VPNs) to circumvent the ban, the Nigerian office of the Presidency discussed building an Internet firewall with the Cyberspace Administration of China[70]. The ban on Twitter was lifted after it agreed to pay an "applicable tax" and establish a local office in the country.[71]

Senegal – A high-level pronouncement by President Macky Sall in 2021 directed the government to migrate all state data from foreign servers to a national data center funded by the Chinese government,[72] having concluded that the majority of data generated in the country is stored abroad.[73] Senegal appears to be adopting a state-centric vision of digital sovereignty, enabled by China 's investment and equipment from Chinese suppliers. The policy wants to capture the economic value of data and prevent foreign access to it, although it is unclear how it will address the relative lack of national digital champions.

66 Department of Communications and Digital Technologies, "Draft National Data and Cloud Policy," 2021. https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

67 "Rwanda National Data revolution and Big data", 2017 http://statistics.gov.rw/publication/rwanda-national-data-revolution-and-big-data

68 National Information Technology Development Agency, "Nigeria Cloud Computing Policy," 2019 https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf

69 "Nigeria bans Twitter after President's tweet is deleted" 5 June 2021, The New York Times. https://www.nytimes.com/2021/06/05/world/africa/nigeria-twitter-president.html

70 Socrates Mbamalu, "Presidency Meets With China's Cyber Regulator to Build Nigerian Internet Firewall," 6 June 2021, Foundation for Investigative Journalism https://fij.ng/article/exclusive-presidency-meets-with-chinas-cyber-regulator-to-build-nigerian-internet-firewall/

71 Adeyemi Adepetun, "Nigeria, Twitter agreement risks collapse over global restructuring," 8 November 2022, The Guardian. https://guardian.ng/news/nigeria-twitter-agreement-risks-collapse-over-global-restructuring/

72 "Senegal aims for digital sovereignty with new China-backed data centre" Reuters, 22 June 2021 https://www.reuters.com/article/senegal-datacenter-idINL5N2O44D3

73 "Le Sénégal ouvre un centre de données national au nom de la «souveraineté numérique," Le Figaro, 22 June 2021 https://www.lefigaro.fr/flash-eco/le-senegal-ouvre-un-centre-de-donnees-national-au-nom-de-la-souverainete-numerique-20210622

C. Europe, Including Russia

European Union – Digital sovereignty in the European Union is a high-level vision that is not directly incorporated in regulatory and legislative proposals, allowing for its fluid application across a wide range of policy objectives. No single agreed term exists within EU policymaking, with "digital sovereignty",[74] "technological sovereignty"[75], and "sovereign European digital economy"[76] all used in strategy documents and public statements without a clear indication of how these terms may differ, if at all. The open-ended nature of digital sovereignty in the EU context lends itself equally to a variety of policy objectives across cybersecurity, economic competitiveness, research, supply chain security, and data protection.

"A Europe Fit for the Digital Age," a 2019 strategy to set the EU's digital agenda, sees the region as a global standards-setter and emphasizes the need to "strengthen its digital sovereignty".[77] The strategy informed the Digital Markets Act (DMA) [78] the Digital Services Act (DSA)[79] the European Chips Act[80].

The 2020 EU Cybersecurity Strategy for the Digital Decade directs investment to mitigate technological and geopolitical risks to EU security. The document calls for "technological sovereignty and leadership",[81] while emphasizing the EU's commitment to the global and open Internet. Among its workstreams is a "European Domain Name System Resolver",[82] so-called DNS4EU, to bolster redundancies in global Internet infrastructure. These projects[83] are intended for voluntary use to create resilience and complement existing global options. These proposals point to a multi-faceted picture of digital sovereignty that can be divided into four themes:

---

74 European Commission, 'A Europe fit for the digital age Empowering people with a new generation of technologies', https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

75 European Commission, 'JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade', https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN

76 European Commission, 'Data Act: Commission proposes measures for a fair and innovative data economy', https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

77 European Commission, 'A Europe fit for the digital age Empowering people with a new generation of technologies', https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

78 European Commission, 'Digital Markets Act', https://competition-policy.ec.europa.eu/sectors/ict/dma_en

79 European Commission, 'Digital Services Act Package', https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

80 European Commission, 'The European Chips Act, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

81 European Commission, 'The EU Cybersecurity Strategy', https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

82 European Union, 'Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade', https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN

83 European Commission, Funding and Tender Opportunities, 'Equipping backbone networks with high-performance and secure DNS resolution infrastructures - Works TOPIC ID: CEF-DIG-2021-CLOUD-DNS-WORKS', https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works

Economic competition: The DMA and DSA aim to reduce dominance in technology markets, typically by US firms operating at the application layer, including social media, search, and messaging. Digital sovereignty here means creating the conditions for European companies to compete with established foreign providers, both to maintain Europe's global influence and guarantee fundamental rights for its citizens. In this framing, digital sovereignty means Europe's ability to grow its own digital providers for the region to determine its own future.

Supply chain resilience: Measures like the European Chip Act and DNS4EU respond to the concern that over-reliance on foreign providers in the supply chain and infrastructure provision is a strategic vulnerability. The European Chip Act aims to reduce dependence on semiconductor chips from abroad, primarily from China and Taiwan. The DNS4EU tender aims to create a voluntary European Domain Name System resolver as an alternative to the largest global services most providers currently use, and which some believe could be chokepoints to access in a significant attack. However, in addition to blocking material such as phishing and malware, as other DNS resolvers routinely do, the tender also requires potential providers to block 'illegal content' across the entire continent.[84] We note that DNS filtering has potentially substantial drawbacks, which should be taken into consideration when developing policy. [85]

Protection against cyberattack: The EU Cybersecurity Strategy[86] is embodied in measures such as the updated Network and Information Security (NIS2) Directive[87] to set up a common level of security and digital infrastructure resilience in all member-states, along with a network of operations centers that form a 'cybersecurity shield' for early detection of cyberattacks.

Empowerment of the individual: The DSA aims to provide "greater democratic control and oversight over systemic platforms".[88] DNS4EU wants to provide DNS resolution by EU-based providers that respect user data privacy, by preventing the monetization of Europeans' DNS

84 Ernesto Van der Sar, 'The EU Wants Its Own DNS Resolver that Can Block 'Unlawful', Traffic, 19 January 2022 https://torrentfreak.com/the-eu-wants-its-own-dns-resolver-that-can-block-unlawful-traffic-220119/

85 The Internet Society, 'Internet Society Perspectives on Domain Name System (DNS) Filtering:', https://www.internetsociety.org/wp-content/uploads/2018/10/Perspectives-on-Domain-Name-System-Filtering-en.pdf

86 European Commission, 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient', https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

87 Thinktank, European Parliament briefing, The NIS2 Directive: A high common level of cybersecurity in the EU', https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

88 European Commission, 'The Digital Services Act: ensuring a safe and accountable online environment', https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

queries. Policymakers often connect this concept of digital sovereignty with "surveillance capitalism"[89] and point to a need to reset the balance of power between citizens and firms.[90]

Digital sovereignty in the EU has different meanings, applications, and goals. As the EU is a significant economic and political power in its own right, in multilateral meetings including the G7 and G20, and through the export of its regulations via "the Brussels effect,"[91] these framings may be globally influential.

EU Member States: France, Germany, and Italy – France and Germany are early drivers of digital sovereignty within the European Union and are quickly being followed by Italy, which uses similar rhetoric. The French-German 2020 Gaia-X joint position paper wants a "sovereign data infrastructure" for EU member states to exchange data safely and securely. It treats the increased volume of data shared and processed between European companies as a source of innovation, value, and competitiveness in the global digital market".[92] It also alludes to individual sovereignty and references the increased ability of "users [to] retain sovereignty over their data".[93]

Digital sovereignty for Italy is seen through a national security lens. Its 2022 National Cybersecurity Strategy[94] aims to protect against hostile state actor activities, cybercrime, cyber-espionage, and disinformation campaigns that seek to polarize public opinion.

France, Germany, and Italy are large economies, have large populations, and have historically held advantageous positions in "influencing up" to the EU level. Digital sovereignty is no exception to this trend with France and Germany articulating visions for digital sovereignty earlier than the European Commission.

89 "Surveillance capitalism" is a term popularized by Shoshanna Zuboff in her 2014 essay, "A Digital Declaration: Big Data as Surveillance Capitalism" and 2019 book, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power." It refers to an economic system based on the collection and commodification of data about people, for economic profit, leading to the growth of near-monopolistic firms with significant and largely untrammeled global economic, political and social power.

90 https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

91 "The Brussels Effect, How the European Union Influences the World", Anu Bradford, (2020) https://global.oup.com/academic/product/the-brussels-effect-9780190088583?cc=au&lang=en&

92 Franco-German Position on GAIA-X, https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=4

93 GAIA-X, last modified 6 September 2022 https://gaia-x.eu/

94 Government of Italy, 'National Cybersecurity Strategy, 2022-2026, https://www.acn.gov.it/ACN_EN_Strategia.pdf

Russian Federation – The term digital sovereignty was frequently used during the annual Russia/China Safer Internet Forum meetings, including a 2016 intervention by a senator urging provider-level pre-filtering to protect "Russian digital sovereignty."[95]

Digital sovereignty in Russia is framed primarily as state sovereignty in the digital realm, and relevant measures exclusively empower state institutions to protect against real or perceived threats to national security, such as disinformation, terrorist content, and cyberattack from hostile state actors. This approach has resulted in policies that increasingly cut Russia off from the global Internet through the mandating of Russian-built and state-controlled Internet infrastructure.

The 2019 "Sovereign Internet Law"[96] and related "Rules for centralized management of a public communication network"[97] required network operators to provide technical information and access to the regulator, Roskomnadzor,[98] so it could "ensure the operation of Russian Internet resources in the event that Russian telecom operators cannot connect to foreign [DNS] root servers".[99] It allowed the regulator to cut off international connectivity or services (e.g. cloud services) and increased its capability to intercept and block traffic. The concept of a sovereign Internet for Russia is one that cannot be disconnected or disrupted by hostile foreign actors, but its implementation allows for significant control over communication and information flows within Russia. It also mandates the use of technical tools to filter and censor content online in the name of battling "false messages" and terrorist content.[100] [101]

Indirectly, the German Council on Foreign Relations has drawn a conceptual link[102] between Russia's understanding of digital sovereignty and the 2014 Amended Data Localization Law,[103] as well as Russia's 2016 "Yarovaya Laws" which introduced mass-surveillance capabilities in the name of combatting terrorism and other "ideologies" online.[104]

---

95 Safe Internet Forum, Russia, 'Moscow Safer Internet Forum adopts Russia-China cybersecurity cooperation roadmap', 19 April 2021, https://safeinternetforum.ru/en/novosti/moscow-safer-internet-forum-adopts-russia-china-cybersecurity-cooperation-roadmap.html

96 "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection'", 22 April 2019, http://publication.pravo.gov.ru/Document/Text/0001201905010025.

97 Rules for centralized management of a public communication network, approved by the Government Decree from 12 February 2020 N 127: Правила централизованного управления сетью связи общего пользования

98 The Federal Service for Supervision of Communications, Information Technology, and Mass Media

99 'Принят закон о «суверенном интернете»', http://duma.gov.ru/news/44551/

100 'Федеральный закон от 06.07.2016 г. № 374-ФЗ', http://kremlin.ru/acts/bank/41108

101 'Федеральный закон от 06.07.2016 г. № 375-ФЗ', http://kremlin.ru/acts/bank/41113

102 Alena Epifanova and Philipp Dietrich, DGAP, German Council on Foreign Relations, 'Russia's Quest for Digital Sovereignty Ambitions, Realities, and Its Place in the World', https://dgap.org/en/research/publications/russias-quest-digital-sovereignty

103 https://pd.rkn.gov.ru/authority/p146/p191/

104 Alena Epifanova and Philipp Dietrich, DGAP, German Council on Foreign Relations, 'Russia's Quest for Digital Sovereignty Ambitions, Realities, and Its Place in the World', https://dgap.org/en/research/publications/russias-quest-digital-sovereignty

Russia's concept of digital sovereignty is significant because it advocates its vision of direct state control of the Internet in key governance bodies such as the International Telecommunication Union. As the concept of digital sovereignty gains traction around the world, Russia may use these organizations to influence Internet regulation globally. It also has regional clout. Russia — along with China —has a direct influence on Eurasian members including Kazakhstan, Kyrgyzstan, and Tajikistan, through the Shanghai Cooperation Organisation. The organization's 2015 cyber-security cooperation agreement aims to limit the use of technologies designed "to interfere in the internal affairs of states; undermine sovereignty, political, economic and social stability; [and] disturb public order."[105]

105 https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/

Appendix II — The Internet Way of Networking

The Internet Way of Networking

Critical Property	Benefits
1. An Accessible Infrastructure with a Common Protocol that is open and has low barriers to entry	Unrestricted access and common protocols deliver global connectivity and encourage the network to grow. As more and more participants connect, the value of the Internet increases for everyone.
2. Open Architecture of Interoperable and Reusable Building Blocks based on open standards development processes voluntarily adopted by a user community	Open architecture creates common interoperable services, which deliver fast and permissionless innovation everywhere. The inclusive standardization process and demand-driven adoption ensures that useful changes are adopted, while unnecessary ones disappear.
3. Decentralized Management and a Single Distributed Routing System which is scalable and agile	Distributed routing delivers a resilient and adaptable network of autonomous networks, allowing for local optimizations while maintaining worldwide connectivity.
4. Common Global Identifiers which are unambiguous and universal	A common identifier set delivers consistent addressability and a coherent view of the entire network, without fragmentation or fractures.
5. A Technology Neutral, General-Purpose Network which is simple and adaptable	Generality delivers flexibility. The Internet continuously serves a diverse and constantly evolving community of users and applications. It does not require significant changes to support this dynamic environment.

For more information about how to do an Internet Impact Assessment, please consult our online guide: **How to Conduct an Internet Impact Brief** using the **Internet Impact Assessment Toolkit.**[106]

106 The Internet Society, 'How to Conduct an Internet Impact - Brief Internet Impact Assessment Toolkit', https://www.internetsociety.org/resources/doc/2021/how-to-conduct-an-internet-impact-brief/

Enablers of an Open, Globally Connected, Secure, and Trustworthy Internet

Supporting an Open Internet	
Easy and unrestricted access	It is easy to become part of the Internet, for networks and users alike. That means that for users the Internet is affordable and Internet services are accessible, and that networks can easily become part of the Internet, without unnecessary regulatory or commercial barriers for both groups.
Unrestricted use and deployment of Internet technologies	The Internet's technologies and standards are available for adoption without restriction. This enabler extends to end-points: the technologies used to connect to and use the Internet do not require permission from a third party, operating system (OS) vendor, a network provider, or any other third party. The Internet's infrastructure is available as a resource to anyone who wishes to use it. Existing technologies can be mixed in and used to create new products and services that extend the Internet's capabilities.
Collaborative development, management, and governance	The Internet's technologies and standards are developed, managed, and governed in an open and collaborative way. This open collaboration extends to the building and operation of the Internet and services built on top of the Internet. The development and maintenance process is based on transparency and consensus, and has as its goal the optimization of infrastructure and services to the benefit of the users of these technologies.
Supporting a Globally Connected Internet	
Unrestricted reachability	Internet users have access to all resources and technologies made available on the Internet and are able to make resources available themselves. Once a resource has been made available in some way by its owner, there is no blocking of legitimate use and access to that resource by third parties.
Available capacity	The capacity of the Internet is sufficient to meet user demand. No one expects the capacity of the Internet to be infinite, but there is enough connection capacity — ports, bandwidth, services — to meet the demands of the users.

Supporting a Secure Internet	
Data confidentiality of information, devices, and applications	Data confidentiality, usually accomplished with tools such as encryption, allows end users to send sensitive information across the Internet so that eavesdroppers and attackers cannot see the content or know who is communicating. Allowing the transfer of sensitive information helps create a secure Internet. Data confidentiality also extends to data-at-rest in applications and on devices. (N.B., "confidentiality" also contributes to privacy, which is part of a trustworthy Internet)
Integrity of information, applications, and services	The integrity of data sent over the Internet, and stored in applications, is not compromised. That is, information sent over the Internet shouldn't be modified in transit, unless directed by the communicating parties (e.g., a captioning bot may be useful to turn spoken words into text).
Supporting a Trustworthy Internet	
Reliability, resilience, and availability	The Internet is reliable when technology and processes are in place that permit the delivery of services as promised. If, for example, an Internet service's availability is unpredictable, then users will observe this as unreliable. This can reduce trust not just in one single service, but in the Internet itself. Resilience is related to reliability: a resilient Internet maintains an acceptable level of service even in the face of errors, malicious behavior, and other challenges to its normal operations
Accountability	Accountability on the Internet gives users the assurance that organizations and institutions they interact with are directly or indirectly acting in a transparent and fair way. In an accountable Internet, entities, services, and information can be identified and the organizations involved will be held responsible for their actions.
Privacy	Privacy on the Internet is the ability of individuals and groups to be able to understand and control what information about them is being collected and how, and to control how this is used and shared. Privacy often includes aspects of anonymity, removing linkages between data, devices, and communications sessions and the identities of the people to which they pertain.

For more information about how to do an Internet Impact Assessment, please consult our online guide: **How to Conduct an Internet Impact Brief** using the **Internet Impact Assessment Toolkit**.[107]

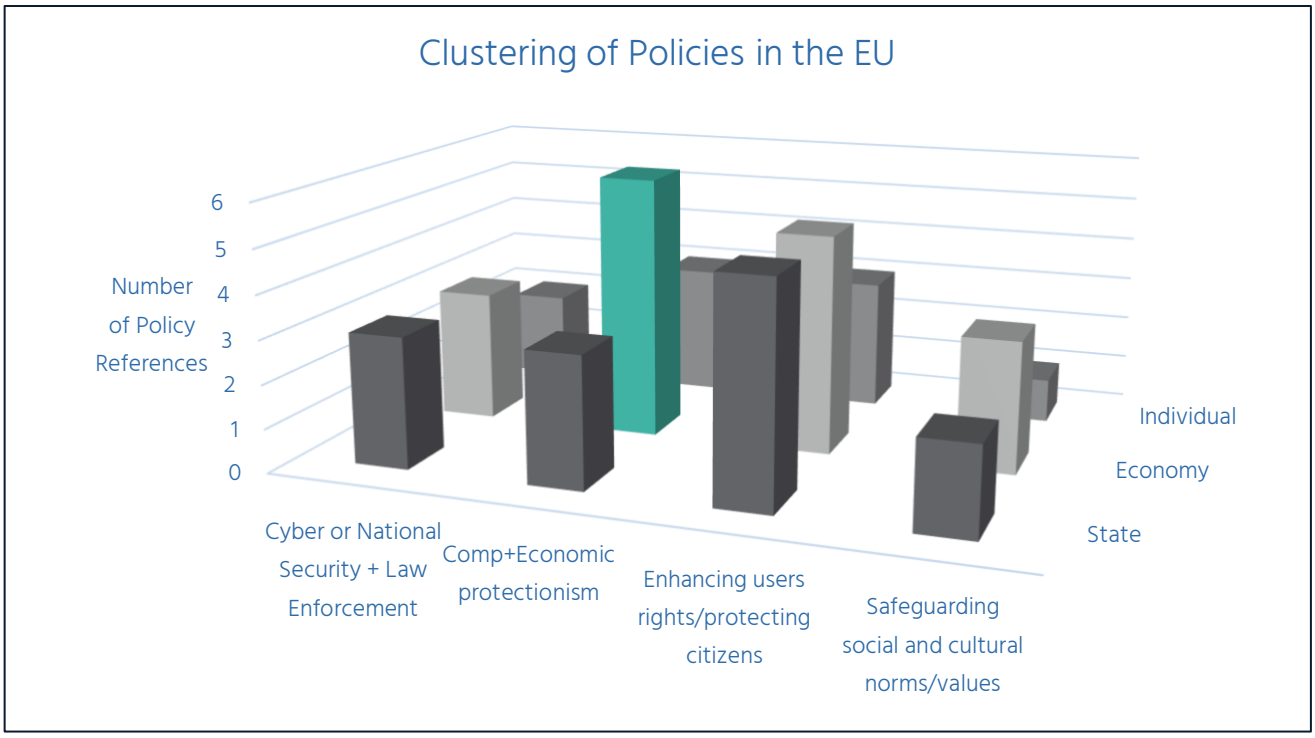
Appendix III — Research Methodology for Digital Sovereignty Types

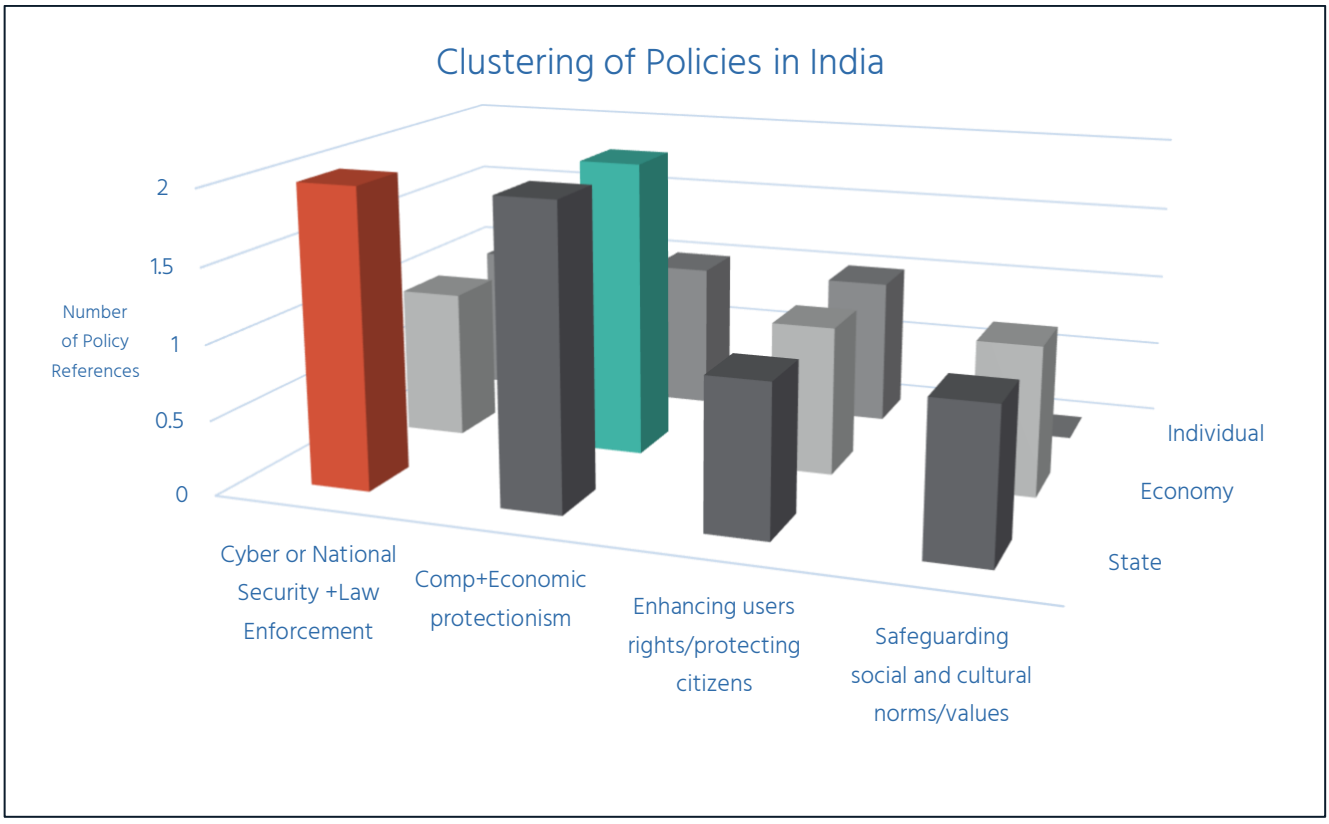
This study analyzed thirty-four policies across three regions based on the two, cross-cutting categories of policy objectives and empowered actors. Each policy is plotted on the chart based on what (a) it wants to achieve, and (b) who it empowers to achieve the policy. For example, if a policy has National Security goal and empowers the State, we add one point to the cell National Security*State. If the same policy also empowers the individual, we add one point to the cell National Security*Individual. If another policy in this jurisdiction also has National Security goal and empowers the State, we add another point to the corresponding cell and sum it up to 2.

The graph immediately below shows that policies are clustered in distinct areas, according to their objectives. Analyzing these clusters by empowered entities showed even tighter clusters which allowed us to identify the key policy types; a distinct cluster of policies fall into National Security/State and Law enforcement/State cells, while policies in the "economy-focused" type are more centered on Competition/Economy and Norms/Society). It is important to note that some of the countries show a mix of the two dominant types, while others have one type standing out. The first graph shows several countries where these patterns and corresponding types are most visible.

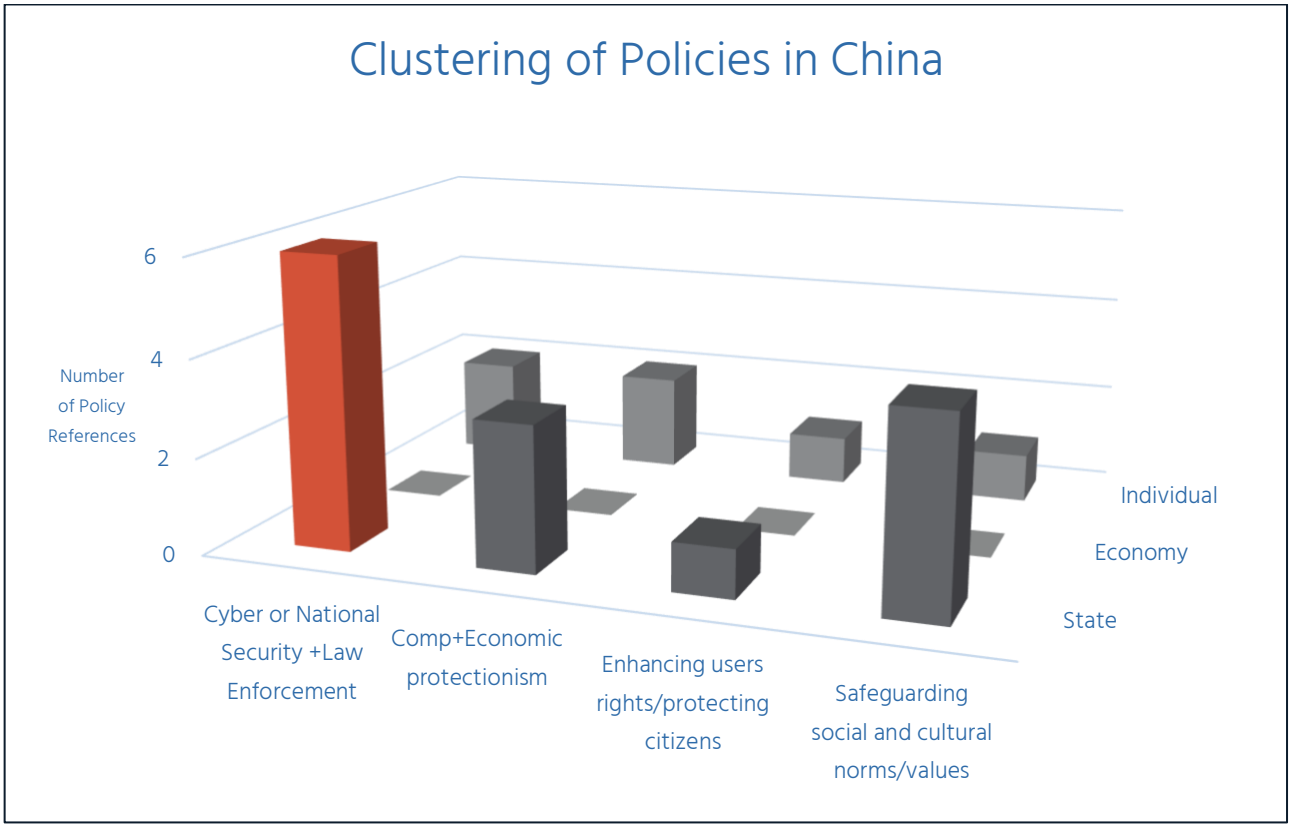
107 The Internet Society, 'How to Conduct an Internet Impact - Brief Internet Impact Assessment Toolkit', https://www.internetsociety.org/resources/doc/2021/how-to-conduct-an-internet-impact-brief/

Policy patterns in different countries exposing 2 distinct types of digital sovereignty, marked in red and green.






Clustering of Policies in Russia
Number of Policy References
4
3
2
1
0
Cyber or National Security + Law Enforcement
Comp+Economic protectionism
Enhancing users rights/protecting citizens
Safeguarding social and cultural norms/values
Individual
Economy
State


Clustering of Policies in China
Number of Policy References
6
4
2
0
Cyber or National Security +Law Enforcement
Comp+Economic protectionism
Enhancing users rights/protecting citizens
Safeguarding social and cultural norms/values
Individual
Economy
State

Appendix IV — Tables of Policies and Proposals Analyzed

Policies of the National Security Type

National Security and rule of law by State
Africa Digital Transformation Strategy (2020 -2030)
African Union - Malabo Convention - Convention on Cyber Security and Personal Data Protection
Australia - Cyber Security Strategy (2020)
Australia - Digital Transformation Strategy (2018)
Australia - Hosting Certification Framework (2021)
China - International Strategy of Cooperation on Cyberspace (2017)
China - Personal Information Protection Law (2021)
China Internet Domain Name Regulations (2017)
China- Cybersecurity Law (2017)
China- Data Security Law (2021)
EU - Data Act (Proposed 2022)
EU - The EU's Cybersecurity Strategy for the Digital Decade (2020)
EU - Digital Services Act (Proposed - 2022)
India - CERT-In Cybersecurity Directions
India - Data Protection Bill (2021)
Indonesia - Government Regulation (71/2019)
Italy - National Cyber Security Strategy (2022)
Russia - "Yaroavaya Laws" (2016): Federal Law "On Combating Terrorism" & "Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation"
Russia - Data Localization Law (2014 amendment)
Russia - Rules for the centralized management of a public communication network (2019), widely known as "Russia's Sovereign Internet Law"
Rwanda - Data Revolution Policy (2017)
South Africa - National Data and Cloud Policy (proposed)
Viet Nam - Law on Cybersecurity (2018)
Viet Nam - Setting up of the Cyber Command (2018)

Policies of the Strengthening the Economy Type

Strengthening economy through competition
African Union - Africa Digital Transformation Strategy (2020 -2030)
EU - Data Act (Proposed — 2022)
EU - Data Act, comments from Thierry Breton, Commissioner for Internal Market
EU - Digital Markets Act (Proposed — 2022)
EU - European Cloud (EC President Ursula von der Leyen 2020 state of union speech) (2020)
EU - GAIA-X (2020)
EU - Shaping Europe's digital future (2019)
India: Data Centre Policy (2020)
India: Data Protection Bill, (2021)
Nigeria - Cloud Computing Policy (2019)
South Africa - National Data and Cloud Policy (Proposed)