Higher National School of Political Sciences

Departement of International Relations

Digital Sovereignty in the Era of Artificial Intelligence : Conceptual Challenges and Necessary Theoretical and Practical Changes

A Dissertation Submitted in Partial fulfillment of The Requirements for Master's Degree in International Relations.

Submitted by :

Lyna Bedairia

Supervised by :

Professor Messiheddine Tassadit

Jury Board

Dr. Nadjoua Bouzourine	PRESIDENT
Dr. Tassadit Messiheddine	SUPERVISOR
Dr. Hichem Daoud ElGhandja	EXAMINER

Academic Year : 2025/2026

Dedication

To my grandfather Noureddine, whose absence was deeply felt throughout this journey, yet whose presence never truly left.

To my parents, for being my constant source of strength, support and encouragement throughout this journey.

To my sisters, Soumia,Meriem,Hanene,Karima, and to my brother Abderraouf, for being my source of motivation.

I am equally grateful for my friends: Thana, Meriem, Aya,Yuki, Ikram, Saliha Noujoud ,Chakira and Hassna for their constant support.

And finally, to those who once doubted me: thank you for pushing me to grow stronger, and believe more in myself.

Acknowledgment

I would like to express my sincere gratitude to my supervisor Professor Messiheddine Tassadit for her guidance.

Special thanks to Dr. Ines benabbes and Dr.Djallel Aimar.

Abstract

This thesis examines how artificial intelligence reconfigures the concept of sovereignty in the digital age. As digital infrastructures, data flows, and algorithmic systems expand across borders, sovereignty is no longer limited to territorial authority alone.

The study analyzes how AI redistributes power between states and technological corporations, creates new forms of digital dependence, and intensifies geopolitical rivalries, particularly between the United States and China. It also explores national and international responses and strategies aimed at asserting digital sovereignty, including AI governance frameworks, cybersecurity measures, sovereign AI initiatives, and data localization policies.

Thus, in the era of artificial intelligence, digital sovereignty requires reconceptualization, as it is increasingly reconfigured into infrastructural, computational, and hybrid forms of authority.

Key words: Artificial Intelligence (AI), Digital Sovereignty, Geopolitics, Data Governance, Cybersecurity.

.

الملخص

تبحث هذه المذكرة في كيفية إعادة تشكيل الذكاء الاصطناعي لمفهوم السيادة في العصر الرقمي. فمع توسّع البُنى التحتية الرقمية، وتدفقات البيانات، والأنظمة الخوارزمية عبر الحدود، لم تعد السيادة مقتصرة على السلطة الإقليمية فحسب.

وهي بذلك تحلل الكيفية التي يُعيد بها الذكاء الاصطناعي توزيع القوة بين الدول والشركات التكنولوجية، ليُنشئ أشكالًا جديدة من الاعتماد الرقمي، ويُكثّف التنافسات الجيوسياسية، ولا سيما بين الولايات المتحدة والصين. كما تستكشف المذكرة الاستجابات والاستراتيجيات الوطنية والدولية الرامية إلى ترسيخ السيادة الرقمية، بما في ذلك أطر حوكمة الذكاء الاصطناعي، وتدابير الأمن السيبراني، ومبادرات الذكاء الاصطناعي السيادي، وسياسات توطين البيانات.

وعليه، ففي عصر الذكاء الاصطناعي، تتطلب السيادة الرقمية إعادةَ المفهمة، إذ تتم إعادة تشكيلها باستمرار ضمن الأشكال البنيوية والحوسبية والهجينة للسلطة.

الكلمات المفتاحية: الذكاء الاصطناعي، السيادة الرقمية، الجيوبولتيك، حوكمة البيانات، الأمن السيبراني

Table of Contents

Dedication ..... **III**

Acknowledgment ..... **IV**

Abstract ..... **V**

Table of Contents ..... **VII**

List of Figures ..... **IX**

List of Tables ..... **X**

List of Acronyms ..... **X**

1. General Background **1**

2. Problem Statement **1**

3.Literature Review: **2**

4.Research Question **2**

5. Hypotheses **3**

6. Objectives of the Study **3**

7.Significance of the Study **3**

8. Factors Influencing Topic Selection **1**

9. Scope and Delimitation **4**

10. Methodological Overview **4**

11. Structure of the Study **5**

PART ONE: Conceptual and Theoretical Framework **6**

1. Foundations of Classical Sovereignty **7**

1.1. Historical and Conceptual Framework **7**

1.1.1 The Evolution and Definition of Sovereignty 7

1.1.2. Typologies of sovereignty: 11

1.1.3. Globalization and the Limits of State Sovereignty 12

1.2. Rethinking Sovereignty In The Digital Age : **15**

1.2.1 .The Rise of Extraterritorial Networks 15

1.2.2.The Development of Cyberspace: 16

1.2.3. Definition and dimensions of digital sovereignty 17

- The Foundations of Digital Sovereignty: **18**

- Dimensions of digital sovereignty : **20**

- Can a State Claim Full Control over Digital Sovereignty ? **25**

1.3.Theoretical Perspectives in International Relations **26**

1.3.1.Digital Sovereignty Through the Lenses of IR Theories: 26

1.3.2.The Need for a New Hybrid Theoretical Framework : 30

PART TWO : Artificial Intelligence and the Reconfiguration of Sovereignty **34**

2. Artificial Intelligence as a Geopolitical and Infrastructural Transformation 35
2.1. Artificial Intelligence as a New structure of Power.....35
2.1.1. The Development of Technology and Artificial Intelligence.....35
2.1.2. Conceptualizing Artificial Intelligence as a Transformative Power:.....37
Related concepts:.....38
2.1.3.Data as a New Raw Material 39
2.2. The reconfiguration of digital sovereignty in the AI era 41
2.2.1. Erosion of territorial sovereignty 41
2.2.2. The Redistribution of Authority Between States and Corporations in the AI Era 43
2.2.3. Digital sovereignty Reconfigured: Authority, Accountabiliy and Democratic issues 46
2.3.Global Power Asymmetries and Digital Dependency 48
2.3.1. Technological Rivalries between U.S and China.....48
The Dimensions of Rivalry- A Comparative Overview :.....48
The United States Strategy: 52
China's Strategy : 52
Towards a Digital Thucydides Trap?.....54
2.3.2. Structural Inequalities and Digital Dependency.....54
***PART THREE : Policy Responses and Practical Transformations*.....60**
3. Digital Sovereignty in Practice: AI Governance and Strategic Responses.....61
3.1. National, Regional and Global Responses: Asserting Digital Sovereignty From Within.....61
3.1.1. National AI Strategies and Digital Sovereignty Models 61
- National AI Strategies :.....64
3.1.2. Regional and Global AI Strategies 67
3.1.3.Global AI Strategies 70
3.2.Sovereign AI, Data Localization and Cybersecurity.....71
3.2.1. Sovereign AI 71
3.2.2.Data Localization 74
3.2.3. Cybersecurity 77
3.3.Toward a New Model of Digital Sovereignty.....79
3.3.1. The limits of Current Responses.....79
3.3.2. Policy Recommendations for the Global South 82

List of Figures

Figure 1 : submarine cables.....22
Figure 2 : Changes in global data flow between regions 23
Figure 3: Global private investment in AI by geographic area,2025 49
Figure 4 : Number of newly funded AI companies by geographic area,2025.....49
Figure 5 : Global private investment in generative AI by geographic area,2019-25.....50
Figure 6 : Countries by model membership. 63
Figure 7. Visualising China's AIDP.....66
Figure 8 . Focus areas and action areas for the AI Strategy:.....69
Figure 9 . A typology of data localization measures and requirements for data flow.....75
Figure 10 . Data localization is growing and becoming more restrictive.....76
Figure 11. Generative AI's Shift 81

List of Tables

Table 1. Composition of Digital Dependence Index DDI.....56
Table 2. Four degrees of digital dependence 57
Table 3 : Construction of Models from codes.....62

List of Acronyms

4IR four Industrial Revolutions
5G *: Fifth Generation of Cellular Network Technology*
AI *: Artificial Intelligence*
AIDP *: Artificial Intelligence Development Plan*
ALPAC *: Automatic Language Processing Advisory Committee*
ANSNET *: Advanced Networks and Services Networks*
APIs *: application programming interfaces*
ARPANET *Advanced Research Projects Agency*
ASEAN *: Association of the Southeast Asian Nations*
ASML *: Advanced Semiconductor Materials Lithography*
AWS *: Amazon Web Services*
CJEU *:Court of Justice of the European Union*
CPS *: Cyber-Physical Systems*
CPST *Cyber-Physical-Social-Thinking*
DDI *: Digital Dependency Index*
DUV *: Deep Ultraviolet*
EU *: European Union*
EUV *: Extreme Ultraviolet Imager*
GAFAM *: Google, Amazon, Facebook, Apple, and Microsoft*
GDPR *: European Union's General Data Protection Regulation*
GPT *: Generative Pre-trained Transformer*
GPU *: Graphic processing unit*
ICANN *: Internet Corporation for Assigned Names and Numbers*
ICC *: International Criminal Court*
ICT *: Information and Communication Technologies*
IEEE *: Institute of Electrical and Electronics Engineers*
IMF *:International Monetary Fund*
IoP *: Internet of People*
IoT *:Internet of Things*
IoTk *: Internet of Thinking*
IPE *: International Political Economy*
IT *: Information Technology*
LLM *: Large Language Models*
MILNET *:Military Network*
MIT *: Massachsetts Institute of Technology*
ML *Machine Learning*

NA North America
NAS *: National Artificial Intelligence Strategies*
NGOs *Non-Governmental Organizations*
NIS *: Network and Information Security Directive*
NSA *: National Security Agency*
NSFNET *: National Science Foundation Network*
OECD *: Organization for Economic Cooperation and Development*
OPEC *: Organization of Petroleum Exporting Countries*
OS *: Operating System*
RuNet *: Russian National Internet Network*
SCCs *: Standard Contractual Clauses*
SMEE *: Shenghai Micro Electronics Equipment*
SMICA *: Semiconductor Manufacturing International Corporation*
Tbps *: Terabits per second*
TCP/IP *: Transmission Control Protocol/ Internet Protocol*
TSMC *: Taiwan Semiconductor Manufacturing Company*
UN *:United Nations*
UNCTAD *:United Nations Conference on Trade and Development*
UNESCO *: United Nations Educational,Scientific and Cultural Organization*
VK *: VKontakte*
WTO *:World Trade Organization*
XCON *Expert Configure*

Introduction

1. General Background

The concept of sovereignty has historically been anchored in the Westphalian ideal of exclusive territorial control and non-interference, established in the 17th century. This classical model defined sovereignty as the absolute and perpetual power of a state within its physical borders. However, the rise of the digital era and the information revolution have rendered these physical borders increasingly permeable. The development of cyberspace—a "CyberPhysicalSocialThinking (CPST) hyperspace"—has blurred the boundaries between digital, physical, social, and cognitive realms, challenging the traditional link between territory and authority.

2. Problem Statement

As digital infrastructures, data flows, and algorithmic systems expand across borders, sovereignty is no longer limited to territorial authority alone. The emergence of **Artificial Intelligence (AI)** acts as a transformative power that reconfigures the foundations of political authority. States now find themselves in a "security dilemma" where reliance on foreign-owned AI systems, cloud providers, and semiconductor supply chains creates structural vulnerabilities. This shift has led to what scholars describe as a "crisis of sovereignty," characterized by a tension between the state's normative status and its practical exercise of power in a globalized digital market.

3. Literature Review

Sovereignty has traditionally been understood as the supreme authority within a defined territory. Classical thinkers such as Jean Bodin and Thomas Hobbes defined sovereignty as absolute, centralized, and indivisible power necessary for ensuring order and stability. Later thinkers, including John Locke, Jean-Jacques Rousseau, and Carl Schmitt, introduced important nuances such as legitimacy, popular sovereignty, and decision-making under exception, but largely preserved the state-centric and territorial conception of sovereignty.

Other scholars challenge this classical view by emphasizing globalization and interdependence. Stephen Krasner, in *Sovereignty: Organized Hypocrisy* (1999), argues that sovereignty has never been fully absolute and defines it as “organized hypocrisy,” shaped by political interests and practical constraints. While this perspective highlights the flexibility of sovereignty in practice, it does not fully move beyond the centrality of the state nor does it account for the structural transformations brought by digital technologies.

More recent scholarship shifts attention toward economic and technological power. Shoshana Zuboff, in *The Age of Surveillance Capitalism* (2019), and Nick Srnicek, in *Platform Capitalism* (2016), emphasize the rise of digital platforms and the concentration of power in technology corporations, where control over data and infrastructures becomes a key source of authority. Extending this argument, Benjamin H. Bratton, in *The Stack: On Software and Sovereignty*

(2015), conceptualizes global computational systems as new architectures of governance, suggesting that sovereignty is increasingly shaped by technological layers that transcend territorial boundaries.

More recent contributions focus specifically on artificial intelligence as a new driver of power. Kate Crawford, in *Atlas of AI* (2021), demonstrates that AI systems are embedded in global networks of extraction, labor, and control, highlighting their political and economic dimensions. However, most of this literature focuses on socio-economic or ethical implications without fully integrating AI into broader theories of sovereignty.

Taken together, these bodies of literature reveal an important gap: while classical and globalization-oriented approaches examine sovereignty evolution, and technological approaches highlight digital power, few studies integrate these perspectives to explain how artificial intelligence reconfigures sovereignty in a systematic way.

This thesis addresses this gap by analyzing how AI reshapes sovereignty through changes in power distribution, control mechanisms, and global asymmetries.

4.Research Question:

How does the rise of artificial intelligence challenge the traditional concept of sovereignty, and what theoretical and practical transformations are required to adapt sovereignty to the digital age?

Subordinate questions explore:

- How do traditional conceptions of sovereignty account for authority in the AI era?
- How effectively do existing International Relations theories explain the emergence and exercise of digital sovereignty in the age of artificial intelligence?
- How effective are current governance mechanisms in preserving state autonomy within an AI-driven and digitally interconnected environment?

5.Hypotheses

Main Hypothesis

Artificial intelligence reshapes sovereignty by redistributing control over data, decision-making, and infrastructures from states to transnational technological actors, requiring a conceptual and practical reconfiguration of digital sovereignty.

Sub-hypotheses

- Traditional sovereignty definitions fail to capture decentralized and algorithmic authority structures
- Existing IR theories are insufficient alone to explain digital sovereignty

- Current governance mechanisms are inadequate for ensuring state autonomy in the AI era

6. Objectives of the Study

- **General Objective:** To examine the conceptual challenges and the necessary theoretical and practical changes required to understand digital sovereignty in the era of AI.
- **Specific Objectives:**
    - To analyze the evolution of sovereignty from the classical age to the digital era.
    - To conceptualize AI as a new structure of power and investigate its impact on territorial sovereignty.
    - To evaluate national and international strategies—such as data localization, cybersecurity, and "Sovereign AI"—intended to assert digital autonomy.

7. Significance of the Study

This study is significant because it addresses the growing **power asymmetries** in the international system. As data becomes the "new oil," control over the "Stack"—the planetary-scale megastructure of computation—becomes a primary determinant of national power. Understanding these dynamics is crucial for states, particularly in the Global South, attempting to break cycles of "digital colonialism" where they provide raw data while importing algorithmic intelligence.

8.Factors Influencing Topic Selection

- **Self-related factors**

My academic background in International Relations and my growing interest in the relationship between power, authority, and governance motivated the selection of this research topic. Throughout my studies, I developed a strong interest in how technology influences international relations and political institutions, particularly how digital tools and artificial intelligence are reshaping state authority and decision-making processes.

In a world where digital spaces transcend physical boundaries, my academic trajectory led me to critically reconsider traditional concepts of sovereignty, borders, and governmental power. This naturally directed my attention toward the concept of digital sovereignty as a framework for understanding these transformations.

- **Topic-related factors**

This topic responds to major transformations in the international system. Artificial intelligence is no longer merely a technological development; it has become a source of power, influence, and geopolitical competition, shaping new forms of rivalry and global inequality.

At the same time, the growing influence of digital platforms, global data flows, and transnational technology corporations raises fundamental questions about who controls digital space and who exercises authority in the digital world. These developments challenge traditional notions of sovereignty and generate new forms of technological dependency and vulnerability, particularly for developing countries.

The concept of digital sovereignty therefore provides a relevant analytical framework for understanding these transformations, as it integrates political, technological, and governance dimensions. It is thus both timely and directly connected to contemporary global issues related to power, autonomy, development, and inequality in the digital age.

9. Scope and Delimitation

The study focuses on the intersection of AI and sovereignty within the field of International Relations. While it covers global trends, it specifically examines the **U.S.-China rivalry** and the **European Union's** normative responses. The research is limited by the practical difficulty of any state claiming "absolute" digital sovereignty due to the transnational nature of data flows and the concentration of critical resources, like semiconductors, in specific geographic hubs.

10. Methodological Overview

This study adopts a qualitative comparative research design to examine how artificial intelligence reconfigures sovereignty in the digital age. Sovereignty is conceptualized as a dynamic structure shaped by technological infrastructures and power relations.

The research combines descriptive, comparative, and analytical approaches. It compares four models of digital sovereignty (United States, China, European Union, and Global South approaches), selected due to their differing governance logics and their role as key actors in global AI governance.

The analysis is operationalized through five indicators: jurisdictional reach, control over data flows, democratic accountability, structural dependency, and normative authority.

The study relies on qualitative sources such as policy documents, AI strategies, regulatory frameworks, and academic literature, complemented by quantitative reports used for contextual support.

The research adopts a **hybrid theoretical framework** to capture the multi-layered nature of digital sovereignty. This approach integrates:

- **International Political Economy (IPE)** to analyze structural power over data and knowledge.

- **Realism** to understand interstate competition and the AI balance of power.
- **Dependency Theory** to highlight structural inequalities between the center and periphery.
- **Constructivism** to explore how digital identities and norms are socially constructed.

11. Structure of the Study

The thesis is organized into three main parts:

- **Part One (Conceptual and Theoretical Framework):** Traces the historical evolution of sovereignty and establishes the hybrid theoretical framework.
- **Part Two (AI as a New Structure of Power):** Analyzes how AI reconfigures authority between states and corporations and explores global asymmetries and dependencies.
- **Part Three (Strategies for Asserting Sovereignty):** Evaluates national and regional AI strategies, focusing on technical and legislative tools like data localization and cybersecurity.

PART ONE: Conceptual and Theoretical Framework

1. Foundations of Classical Sovereignty

1.1. Historical and Conceptual Framework

To understand the current crisis of sovereignty in the digital era, it is first necessary to establish the conceptual and historical foundations of classical sovereignty, the following section traces this evolution, essential to understand how is sovereignty challenged in the artificial intelligence era.

1.1.1 The Evolution and Definition of Sovereignty

Throughout ancient and medieval history,legitimacy was not a fixed or universal concept but a dynamic interplay between philosophy, religion and politics.In China legitimacy emerged from the fusion of the Mandate of heaven,Confucian ethics,and Legalist discipline, which is a moral and cosmic justification for authority that bound rulers to a high ordert hey could not claim by force alone.In Greece,it was grounded in civic participation, philosophical virtue and mythological narratives that linked rulers to divine sanction.India's conception was deeply spiritual,guided by Dharma as both cosmic compass and an ethical framework for governance.Rome combined mythology,law, and religious symbolism to secure social stability and imperial continuity across a vast and diverse empire.Medivial Europe's legitimacy evolved through feudal hierarchies and Chrisitian theology, while in islamic world,it was anchored in divine law and the caliphate's dual claim to spiritual and temporal leadership.Across these civilizations,legitimacy was never merely a legal arrangement,it was a moral architecture of power,binding rulers to cosmic,ethical, and communal principles that sustained authority and social cohesion[1].

While these civilizations laid diverse foundations for political authority , it was in early modern Europe that sovereignty began to take its modern form; Jens Bartelson divides its history into three distinct periods, arguing that this periodization reflects underlying epistemic shifts that redefined the relationship between knowledge and power[2].

The Renaissance marks what Jens Bartelson describes as a phase of proto-sovereignty. During this period, Europe was still shaped by medieval religious hierarchies, Church supremacy, imperial claims, and feudal fragmentation; however, the intellectual climate was undergoing significant transformation. Niccolò Machiavelli, in *The Prince*, emphasized pragmatic power and the necessity of strong rulers, breaking away from purely theological justifications. Thomas More's *Utopia* envisioned ideal forms of governance, while Francisco de Vitoria examined the legitimacy of conquest and colonial expansion, raising critical questions about imperial authority and the moral limits of political power within the framework of natural law.

[1] Tural Alakbarov, "Sources of the Concept of Legitimacy in the Ancient and Middle Ages," Metafizika Journal 8, no. 1 (2025): 141–153.
[2] Bartelson, *A Genealogy of Sovereignty*, 84.

During this period, sovereignty remained deeply entangled with divine authority and moral order, yet the foundations of secularization were being established. This proto-sovereignty laid the groundwork for later theories by shifting the focus from purely spiritual legitimacy to worldly political necessity.

At the level of knowledge and justification, this period reflects a transition from a predominantly theological worldview to a more human-centered approach. Knowledge was no longer grounded exclusively in divine revelation; it increasingly incorporated classical philosophy, empirical observation, and pragmatic statecraft. Thinkers such as Machiavelli exemplify this transformation, as politics began to be analyzed in terms of power, stability, and strategic necessity rather than solely through moral or religious doctrine.

However, sovereignty in the modern sense had not yet fully crystallized. Political authority remained fragmented among monarchs, city-states, empires, and religious institutions. What emerged during this period was not full sovereignty, but rather its conceptual foundations: the idea that political authority could be centralized, territorially organized, and justified through practical reasoning rather than divine hierarchy alone. This proto-sovereignty thus reflects an epistemic transition from sacred order to political rationality.[1].

- **. The Classical Age (17th Century): Sovereignty and Interest**

At the epistemological level, this period reflects the rise of rationalism, scientific inquiry, and systematic political theory. Knowledge became increasingly structured around reason, order, and systematization.

According to Bartelson, the Peace of Westphalia is frequently mythologised as the origin of sovereignty, but this perspective oversimplifies a far more contentious historical process. Although political entities maintained relations during this period, these interactions were not conceptualized as part of a coherent "international system" in the modern sense.[2] The 1648 treaties did codify two significant concepts that would later become essential to the Westphalian model : the legal equality of nations and the ideal of non-intervention in domestic affairs.

Thomas Hobbes, in *Leviathan*, argued that absolute sovereignty was necessary to prevent chaos and civil war, presenting the sovereign as the guarantor of peace and stability. John Locke, in contrast, emphasized contractual legitimacy, arguing that political authority must be grounded in the consent of the governed and limited by natural rights. Although Locke belonged to the seventeenth century, his theory anticipated later developments toward constitutional and popular sovereignty.

This period also saw the influence of Cartesian rationalism, which reinforced the idea that political authority could be constructed and justified through logical reasoning. Sovereignty thus shifted further away from theological foundations toward rational and secular ones, becoming the cornerstone of modern political philosophy.

The state came to be conceptualized as an artificial yet coherent entity, capable of pursuing its own survival and stability. Sovereignty was now defined as supreme and indivisible authority within a clearly defined territory. It was no longer primarily theological; it was juridical and

[1] Bartelson, *A Genealogy of Sovereignty*, 88,136.
[2] Bartelson, *A Genealogy of Sovereignty*, 137.

political. The sovereign became the ultimate lawgiver and the final authority in matters of internal governance and external independence.

The idea of *raison d'état* (reason of state) illustrates this shift. Political decisions were justified not by divine mandate but by the necessity of preserving order and advancing the interests of the state. Authority became secularized, strategic, and territorially anchored.[1]

- **. Modernity (18th–19th Centuries)**

In the eighteenth and nineteenth centuries, sovereignty underwent another significant transformation. The Enlightenment, the American and French Revolutions, industrialization, and the rise of nationalism reshaped political thought. Sovereignty, while retained as a central principle, was reinterpreted.

Modernity was characterized by the growing authority of reason, science, and the concept of popular will. Legitimacy was no longer anchored solely in monarchical authority or abstract state interest; instead, it increasingly derived from the people. The doctrine of popular sovereignty emerged as a foundational principle.

The sovereign was no longer simply the monarch; it became the nation, the people, as Jean-Jacques Rousseau argued, or the constitutional order. Sovereignty became linked to representation, rights, and constitutional frameworks. While still territorially bounded, it was embedded within new institutional structures such as parliaments and codified legal systems[2].

This phase reflects a transition from sovereignty as centralized absolutism to sovereignty as a principle of collective political identity. Authority became constitutionalized and, in some contexts, democratized.

At the same time, the nineteenth century also witnessed the consolidation of the modern nation-state and the expansion of bureaucratic administration. Later, Max Weber analyzed the modern state as a political organization that successfully claims the monopoly of legitimate physical violence within a given territory, emphasizing the rational-legal institutionalization of authority[3].

Sovereignty reemerged, in the twentieth century, at moments of rupture. Carl Schmitt famously defines the sovereign as "someone who decides on the exception." [4] Sovereignty, in this understanding, is not revealed through periodic legality but through the suspension of it. The ability to decide that normal order no longer applies reveals the ultimate locus of authority.

At the same time, globalization, supranational institutions, economic interdependence, and human rights regimes began to complicate classical territorial sovereignty. Authority became stratified and diffused, and world governance structures limited state autonomy to a degree.

[1] Bartelson, *A Genealogy of Sovereignty*, 137,180.
[2] Bartelson, *A Genealogy of Sovereignty*, 240,254.
[3] Max Weber, *From Max Weber: Essays in Sociology*, trans. and ed. H. H. Gerth and C. Wright Mills (New York: Oxford University Press, 1946), 78.
[4] Schmitt, Political Theology Four Chapters on the Concept of Sovereignty , 9.

- **Epistemological Transitions Across the Phases**

Across these periods, sovereignty evolved alongside shifts in the foundations of knowledge and legitimacy. In the Renaissance, authority began to detach from purely theological justification and move toward pragmatic political reasoning. Later, in the Classical Age, it was systematized through rationalist philosophy and tied to state interest and territorial supremacy. In Modernity, sovereignty was re-legitimized through the concept of the people, constitutional order, and national identity.

Each phase reflects a deeper transformation in how political order is understood: from sacred hierarchy, to rational statehood, to popular and constitutional legitimacy.

This genealogical perspective reveals that sovereignty is not static. It adapts to the dominant epistemological frameworks of each era. Understanding these transitions is essential for analyzing current debates, where globalization and new technological and digital conditions may once again be reshaping the foundations upon which political authority rests.

- **Definition of Sovereignty:**

According to Jean Bodin, sovereignty is the absolute and perpetual power of a republic; it represents the highest authority within the state, from which all other powers derive [1] . In *Leviathan*, Hobbes defines sovereignty as the artificial soul of the commonwealth. He compares the state to an artificial man, with sovereignty functioning as the principle that gives life and motion to the entire political body[2]. Sovereignty, for Hobbes, is absolute and indivisible[3], created through the social contract by which individuals escape the chaotic state of nature. Sovereignty is thus the essential condition for peace and security, since only a unified and supreme authority can prevent disorder.[4]Jean Lock offers a more limited conception. Sovereignty, though established through consent, is conditional and constrained by the protection of natural rights[5]. If authority violates these rights, it loses its legitimacy[6]. . Similarly, Jean-Jacques Rousseau locates sovereignty in the general will of the people [7]. While sovereignty remains absolute, it belongs collectively to the people rather than to a monarch.[8].

Carl Schmitt defined sovereignty as the power to decide on the exception. For Schmitt, sovereignty is ultimately revealed in moments of crisis, when a political authority determines whether the normal legal order should be suspended.[9].

[1] Bodin, *Les six livres de la République*, 74.
[2] Hobbes, *Leviathan*, 8.
[3] Hobbes, *Leviathan*, 160.
[4] Hobbes, *Leviathan*, 153.
[5] Locke, Two Treatises of Government, 106.
[6] Locke Two Treaties of Government, 197.
[7] Rousseau, *Du contrat social ou principes du droit politique*, 23,24.
[8] Rousseau, *Du contrat social ou principes du droit politique*, 31,32.
[9] Schmitt, Political Theology Four Chapters on the Concept of Sovereignty, 9.

Scholars distinguish between *de facto* sovereignty, which is a state's actual ability to exercise power within its borders, and *de jure* sovereignty, which is the official authority recognized by international law and by other governments. *De facto* sovereignty is concerned with actual governance, such as the capacity to enforce laws, collect taxes, provide public services, and maintain security, whereas *de jure* sovereignty represents legitimacy derived from treaties, legal recognition, and normative conventions. This divide explains why a state may be fully recognized in theory but lack effective control in reality. This gap is especially noticeable in the age of digital networks and globalization, where the exercise of authority is sometimes complicated by non-state actors and foreign powers.[1].

Operationally, sovereignty can be defined as the highest and legitimate authority exercised over a political community, traditionally rooted in territorial boundaries. It refers to the capacity to make binding decisions, enforce them, and, when necessary, act decisively in exceptional circumstances without being subject to a superior power. Historically, sovereignty has depended on control over institutions, legal systems, and the practical instruments that allow authority to be effectively exercised.

Yet today, political authority is no longer sustained by territory and institutions alone. It increasingly depends on the regulation of information flows, digital infrastructures, and technological systems that structure economic, social, and political life. As a result, the foundations of sovereignty appear less exclusively territorial and more deeply intertwined with technological and computational infrastructures.

1.1.2. Typologies of sovereignty:

At the international level, legal sovereignty is linked to the mutual recognition between states, in this sense sovereignty depends not only on internal authority but also on external acknowledgement within the international arena. Meanwhile the Westphalian sovereignty, referes to the autonomy of the state and the exclusion of external actors from domestic affairs, yet in practice, such autonomy has been eroded through military intervention, economic pressure or the influence of international institutions. This gap between principle and practice becomes even more apparent when considering domestic sovereignty, which refers to the organization of authority within the state, and its capacity to exercise effective control over its territory and population.

Moreover**, interdependence sovereignty** ; also reffered to as **shared sovereignty,** refers to the state's ability to regulate transborder flows, including people, goods, capital, information and ideas, strongly increased in the context of globalization, as states recognize that certain challenges exceed their individual regulatory capacity and require collective governance arrangements. The EU represents the most advanced examples of shared sovereignty in practice, as member states have voluntarily transferred significant portions of their authority to supranational institutions resulting the backward of national control [2].The world Trade

[1] Pierucci, « Sovereignty in the Digital Era », 2025, 4.
[2] *In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions.* 2026. Leiden University Scholarly Publications, 5.

organization represents another form of shared sovereignty,where states accept policy changes requirements that can erode national policies[1].

However, this type of sovereignty becomes particularly fragile, as economic integration and technological networks limit state's regulatory capacity.

Krasner argues that these kinds of sovereignty do not necessarily coincide, a state may enjoy international recognition while lacking domestic control. It may formally reject external interference while voluntarily accepting constraints through international institutions. Sovereignty, therefore, operates as what he calls"organized hypocrisy":a principle that is universally invoked but selectively applied.[2]

This fragmentation is particularly relevant in the digital age. Interdependence sovereignty is challenged by cross-border data flows and global digital infrastructures. Westphalian sovereignty is complicated by the presence of transnational technology corporations that influence domestic authority structures. Domestic sovereignty is tested when critical digital systems are controlled by private actors rather than the state. Krasner's framework thus provides a useful analytical tool for understanding how sovereignty, already internally differentiated, faces new tensions in the context of digitalization and artificial intelligence.

Beyond the previously mentioned kinds of sovereignty, scholars distinct also **functional sovereignty,**which refers to exercising authority in contested territories, in certain governance functions ,without being fully recognised, at the same time these functions work across borders only if other actors acknowledge them . Kosovo for instance, issues licence plates that other countries accept, Palestine prints postage stamps recognised by the Universal Postal Union. Taiwan manage national Internet domains ".tw". These examples show that sovereignty can operate in fragments with the recognition of particular functions[3].

1.1.3. Globalization and the Limits of State Sovereignty

The origins of contemporary globalization can be traced to the post World War II initiative to stabilize the international economy. At the 1944 Bretton Woods Conference, the Allied powers established a framework aimed at preventing the protectionism and financial instability that had characterized the interwar period. This framework created the International Monetary Fund (IMF) to maintain monetary stability, the World Bank to finance reconstruction and development projects, and the General Agreement on Tariffs and Trade), which later evolved into the World Trade Organization (WTO) in 1995. Together, these bodies provided the rules and mechanisms necessary to expand trade and investment across borders.

For nearly thirty years, this system supported what is often called a "golden age of controlled capitalism." Influenced by John Maynard Keynes, governments in industrialized countries

[1] R. Rao. "The Impact of Global Trade Agreements on National Sovereignty: A Legal Review." *Indian Journal of Law* 2, no. 5 (2024): 7–13.
[2] Krasner, *Sovereignty:Organized Hypocrisy*, 4.
[3]Florea, Adrian, and Reyko Huang. "Functional Sovereignty in Contested Territories." *International Studies Quarterly* 69 (2025) , 2.

combined international economic cooperation with domestic policies that promoted full employment, welfare expansion, and wage growth, creating a temporary social compromise between capital and labor. However, by the early 1970s, the system began to unravel. The United States abandoned the dollar's gold peg in 1971, leading to economic instability characterised by inflation, unemployment, and energy crises. This collapse paved the way to the adoption of new economic ideas.

In the 1980s, leaders such as Margaret Thatcher and Ronald Reagan spearheaded a neoliberal shift, advocating deregulation, privatization, and the liberalization of trade and capital flows. Rooted in the classical liberalism of Adam Smith and David Ricardo, neoliberalism emphasized market efficiency through self-regulation and rejected state intervention. The end of the Cold War further legitimized this model, linking globalization to the worldwide spread of market liberalization.[1]

Since the 1990s, globalization has been defined by three interconnected trends:

- the internationalization of trade and finance,
- the rising influence of transnational corporations and investment banks,
- and the enhanced role of global economic institutions like the IMF, World Bank, and WTO.

These developments transformed globalization from a postwar stability project into a comprehensive process of economic integration, reshaping the interactions among states, markets, and societies.

The authority of governments - whether powerful or weak, large or small- has been eroded by technological shifts and the rapid integration of national economies into a single global market. Their inability to manage domestic economies, sustain employment, maintain growth, balance payments, or control interest and exchange rates is not due to incompetence, corruption, or poor leadership. Nor can these shortcomings be attributed to other states or governments. Instead, they reflect the reality that governments themselves have become subject to the forces of the global market, leaving them more as its victims than its masters[2].

- **Crisis and asymmetry:**

First, state autonomy has decreased as a result of economic interconnectedness, since governments have become more susceptible to changes in international markets, investment flows, and credit systems. Competitiveness and capital flight increasingly limit policy choices in the fiscal, monetary, and industrial domains, integrating national decision-making into international markets. Global networks concentrate flows through a few core hubs, allowing certain states to use interdependence as leverage. At the same time, globalization has produced new structural dynamics. Because of this "weaponized interdependence," power can be used to

[1] Steger, *Globalization*:a very short introduction 52,56.
[2] Strange, The Retreat of the State , 14.

manipulate the architecture of the networks that others rely on, in addition to market size and bilateral pressure[1].

Second, the range of organizations with state-like authority extends beyond the borders of traditional states. Certain international organizations—including the World Trade Organization (WTO), Court of Justice of the European Union (CJEU), World Bank, and International Monetray Fund (IMF)—now exercise significant authority, sometimes even more than some states. Through structural adjustment initiatives in Latin America in the 1980s and 1990s, for instance, these institutions limited national autonomy, marking a shift from the traditional interstate system in which sovereignty was solely territorial. In parallel, supranational governance mechanisms multiplied as states voluntarily accepted binding commitments through trade agreements, financial arrangements, and multilateral institutions. While these commitments were justified as necessary for cooperation, they simultaneously restricted unilateral state action. Authority thus became layered across national and international levels, complicating the classical Westphalian ideal of exclusive territorial control.[2].

Third, the development of international human rights regimes significantly reshaped the normative foundations of sovereignty. The internal treatment of populations increasingly became a matter of international concern, challenging the traditional understanding of sovereignty as absolute and unrestricted authority over domestic affairs. Instead, sovereignty gradually came to be viewed as a form of responsibility embedded within broader international normative frameworks. In this context, new patterns of transnational political influence also emerged, most notably the boomerang pattern[3]**.** This dynamic occurs when domestic groups operating in repressive environments are unable to influence their governments directly and therefore seek support from international allies. By linking with transnational advocacy networks and international organizations, these actors can mobilize external pressure on norm-violating states. Such networks provide domestic groups with access to information, resources, and political leverage, while international partners amplify their demands and reflect them back into the domestic arena, reinforcing growing international scrutiny of state behavior.

Finally, the expansion of information and communication technologies further weakened the traditional linkage between authority and territory. While borders remain politically significant, they have become increasingly permeable to the movement of capital, information, and ideas.

Digital networks enable rapid cross-border exchanges that are difficult for states to fully regulate, challenging their ability to control financial and informational flows. At the same time, the architecture of global information networks creates asymmetries of power. States that control or have privileged access to key network hubs can obtain valuable information about the activities and strategies of other actors. This "panopticon" effect provides them with an informational advantage, allowing them to better interpret the intentions and tactics of their

[1] Farrell et Newman, *Weaponized Interdependence*, 44,47.
[2] Joseph A. Conti, "Supranational Stateness: International Courts and the Globalization of Political Power," Michigan Journal of Law & Society 1 (2007): 18.
[3] Margaret E. Keck and Kathryn Sikkink, Activists beyond Borders: Advocacy Networks in International Politics (Ithaca: Cornell University Press, 1998)., 18.

rivals and to respond strategically through negotiation, political framing, or countermeasures. Consequently, the structure of digital networks does not simply diffuse power; it can also concentrate informational capabilities in the hands of actors positioned at critical points within global infrastructures.[1]

The crisis of sovereignty in the age of globalization does not consist in its disappearance, but in the growing tension between its normative status and its practical exercise. Sovereignty remains the organizing principle of the international system; however, its empirical capacity is mediated by institutional and economic structures.

Moreover, globalization has been marked by significant asymmetries. Although institutions such as the World Trade Organization operate on principles of formal equality, economically powerful states often possess greater negotiating leverage and institutional influence. Wealthier nations command more extensive legal expertise, economic weight, and capacity to shape regulatory standards. Developing states, while formally sovereign and legally recognized, may face structural disadvantages within global trade and financial systems.

Similarly, financial conditionality associated with institutions such as the International Monetary Fund has, at times, constrained domestic policy autonomy. Trade agreements and investor–state dispute mechanisms can allow private actors to challenge national regulations, effectively shifting elements of authority from domestic public institutions to transnational legal frameworks.

Globalization, therefore, does not simply erode sovereignty; it reorganizes it unevenly. Sovereign equality persists as a juridical norm, yet material inequalities shape the capacity of states to exercise meaningful autonomy. These changes demonstrate how global institutional, technological, and economic forces have progressively influenced sovereignty. The emergence of digital infrastructures and artificial intelligence in the modern era marks a new phase in this evolution, posing additional theoretical and practical difficulties for governments attempting to preserve digital sovereignty.

1.2. Rethinking Sovereignty In The Digital Age :

This section focuses on the digital age and the new questions it raises, including whether any state can still claim full and effective control over its own sovereignty. It proceeds by analyzing the rise of extraterritorial networks, the development of cyberspace, the tension between continuity and rupture in sovereign authority, and finally arrives at a working definition of digital sovereignty and its principal dimensions.

1.2.1 .The Rise of Extraterritorial Networks

[1] Farrell et Newman, *Weaponized Interdependence*, 55.

The geographical arrangement of social, political, and economic relations has been significantly altered by the rapid development of digital technologies. A new environment, known as cyberspace, has emerged as a result of the growth of the Internet and international communication networks, enabling the cross-border exchange of goods, services, and economic activity. Unlike traditional political space, which is delimited by national borders and state control, digital space functions through transnational technological infrastructures that connect actors worldwide. Consequently, maintaining the traditional link between territory and sovereignty has become increasingly challenging in the digital age.

1.2.2.The Development of Cyberspace:

The evolution of cyberspace can be traced back to the invention of the first computer in 1946, which marked the beginning of digital computation. By the 1950s, the mass production of computers introduced these machines into everyday life and industrial processes, creating a growing need for interconnected systems. This demand led to the establishment of ARPANET in 1969 by the Advanced Research Projects Agency, a pioneering network that enabled communication between distributed computers and is often regarded as the precursor to the Internet. In the mid-1970s, ARPANET transitioned into a commercial network, embedding principles such as packet switching, decentralized control, and resource sharing[1]. Yet, communication remained confined within single networks until ARPA initiated the "internetwork" project, which introduced Transmission Control Protocol and Internet Protocol TCP/IP and transformed the Internet into an open, scalable system. During the 1980s, NSFNET gradually replaced ARPANET as the backbone of the Internet, while MILNET was separated for military use. ARPANET was officially retired in 1989, symbolizing the Internet's shift from military to civilian applications. The 1990s accelerated this transformation, with corporate initiatives such as ANSNET paving the way for full commercialization by 1995[2]. At this stage, cyberspace was largely synonymous with the Internet, encompassing infrastructures, systems, data, and activities. Subsequent innovations—including Cyber-Physical Systems (CPS), the Internet of Things (IoT), the Internet of People (IoP), and the Internet of Thinking (IoTk)—extended cyberspace beyond digital networks, integrating physical devices, social relations, and human cognition. This convergence ultimately produced the Cyber-Physical-Social-Thinking (CPST) hyperspace, or "general cyberspace," which blurred the boundaries between digital, physical, social, and cognitive realms, reshaping human interaction, governance, and knowledge production[3].

According to Joseph Nye, "cyberspace is an operational domain framed by use of electronics to exploit information via interconnected systems and their associated infrastructure."[4] In this

[1] Ning, *A Brief History of Cyberspace*, 2.
[2] Huansheng Ning, *Cyberspace, Cyber Philosophy, and Cyberlogic: A Brief History of Cyberspace*. Boca Raton: CRC Press, 2023 , 3.
[3] Huansheng Ning, *Cyberspace, Cyber Philosophy, and Cyberlogic: A Brief History of Cyberspace*. Boca Raton: CRC Press, 2023 ,4
[4] Nye, *The Future of Power*, Online-Ausg (PublicAffairs, 2011), 122.

context, cyberspace refers to the digital world that is produced, transported, and processed via international communication networks

Some scholars believe that network organisations will take the place of bureaucratic hierarchies as a result of the Information Revolution. Nonprofit organisations and private markets will perform more governmental tasks. As virtual communities grow on the Internet, they will transcend national borders and create their own government structures[1].

- **Sovereignty in the Scope of Cyberspace : Between Continuity and Rupture :**

Cyberspace introduces a fundamental tension in International Relations: does the decentralisation and fragmentation of authority inherent in digital networks signify the decline of state sovereignty, or rather its reconfiguration within the Westphalian logic of territorial control? While the proliferation of non-state actors, platforms, and transnational flows suggests a dispersion of power, the persistence of state-centric legal and security frameworks points to continuity rather than rupture.

Within this contested arena, two discursive challenges emerged: cyber exceptionalism, which portrayed the internet as an autonomous realm beyond state law and territorially, and multi-stakeholder Internet governance, which advocated collective regulation by governments, companies, civil society, and technical experts, thereby diluting the state's monopoly on authority. Yet, despite these challenges, states have reframed sovereignty as indispensable in the digital age.Through the notion of "digital sovereignty", they have justified renewed control over infrastructure, data, and platforms, positioning themselves as central actors in safeguarding national security, economic independence, and citizens rights[2].

States seek to territorialize cyberspace through data localization, such as Russia’s requirements that personal data of its citizens must be stored on servers inside the country in addition to sovereign internet law ; which refers to the legal frameworks that give governments the authority to control, filter, or even isolate their national segment of the internet, for instace the so-called « RuNet» ; which is the Russian attempt to mainatin a self-contained internet ecosystem.[3] These measures demonstrate that Westphalian logic is extended to cyberspace,producing a reconceptualization of sovereignty rather than a rupture, towards a shared, multi-layered and relational sovereignty, as states project power via laws and infrastructures.

1.2.3. Definition and dimensions of digital sovereignty

[1] Nye, *The Future of Power*, Online-Ausg (PublicAffairs, 2011), 113,114.
[2] Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4): 4,5.
[3] Cybercrime Diaries. “Russia’s Sovereign RuNet – A Challenge to the Cybercrime Underworld?” *Cybercrime Diaries*, accessed April 18, 2026 https://www.cybercrimediaries.com/post/russia-s-sovereign-runet-a-challenge-to-the-cybercrime-underworld.

The ability of a state to govern, manage, and safeguard digital data, infrastructure, and technology under its control is known as **digital sovereignty**. This concept has evolved to encompass control over data, algorithms, platforms, and technological standards in cyberspace, while building on the traditional idea of Westphalian sovereignty. Fundamentally, digital sovereignty refers to a government's capacity to establish regulations for data collection, processing, storage, and transmission, including the ability to impose limitations on cross-border data transfers. Importantly, despite frequent overlaps, digital sovereignty is **not** synonymous with cybersecurity or data protection.

To clarify its scope, it is useful to distinguish digital sovereignty from related concepts. **Cybersecurity** refers to the defense of systems, networks, and data against cyber threats, while **data protection** primarily addresses individuals' rights regarding their personal information. In contrast, digital sovereignty represents a broader political and legal assertion of control over digital ecosystems, encompassing the ability to reduce foreign dependence and influence within the digital domain[1].

Political actors have also helped shape the understanding of digital sovereignty. For example, Charles Michel, President of the European Council, described it as "a means for achieving strategic autonomy, which is about being able to make choices, reducing our dependencies, and better defending our interests and values." [2]

Several scholars have further refined the concept from an analytical standpoint, highlighting its institutional and structural dimensions. Luca Belli, Yuxiang Jiang, and Huw Roberts et al. define digital sovereignty as "the exercise of legitimate authority over digital infrastructure and protocols, emphasizing the necessity for nations to actively influence the digital ecosystem". [3]

Operationally, digital sovereignty refers to a state's ability to reduce strategic reliance on external actors while exercising effective and independent control over digital infrastructures, data flows, and technological systems both within and beyond its borders. This includes not only legislative authority over the collection, processing, and transmission of data but also the capacity to influence technological standards, regulate digital platforms, and safeguard critical infrastructures. In this sense, digital sovereignty is a multifaceted concept that combines legal, technological, and geopolitical dimensions, representing both the continuity of state authority and its evolution in the digital era.

- **The Foundations of Digital Sovereignty:**

[1] Kaya, M., & Shahid, H. (2025). Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. Interdisciplinary Studies in Society, Law, and Politics, 4(2), 219-233 :222 ,223.
[2] Roberts et al., « Safeguarding European Values with Digital Sovereignty », 4.
[3] María del Pilar Rodríguez Pita, Jorge Emiliano Pérez Martínez, and Alberto Urueña López, "From Concept to Method: A Framework for Measuring Digital Sovereignty," paper presented at the *ITS 33rd European Conference 2025: Digital Innovation and Transformation in Uncertain Times*, Edinburgh, June 29–July 1, 2025 (Calgary: International Telecommunications Society, 2025), 11.

The concept of digital sovereignty first appeared in Chinese political and academic discourse at the beginning of the twenty-first century under the term **"cyber sovereignty."** It emerged partly as a response to the expanding global influence of the United States in the digital domain. During the post–Cold War period, the United States promoted the use of information and communication technologies as instruments of "soft power," presenting the internet as a tool for democratization, openness, and liberal economic integration. However, Chinese scholars and policymakers often interpreted this strategy differently, viewing the decentralized and borderless structure of the internet as a mechanism that enabled Western—particularly American—dominance over global digital governance. The United States' considerable influence over key internet governance organizations, such as the **Internet Corporation for Assigned Names and Numbers (ICANN),** which controls crucial elements of the internet's technical infrastructure, reinforced this perception[1].

A similar discussion later arose in Europe, especially in France, where policymakers began promoting the concept of **"digital sovereignty"** in reaction to the increasing power of major American tech firms, commonly referred to as **GAFAM**: Google, Amazon, Facebook, Apple, and Microsoft. European governments considered stronger regulatory frameworks to safeguard strategic technological autonomy due to concerns about economic dependence on these companies and the transfer of digital wealth overseas[2].

The debate intensified following the 2013 global surveillance revelations by Edward Snowden. These disclosures exposed the National Security Agency's (NSA) and its foreign partners' extensive surveillance activities, including the mass collection of data on individuals, governments, and businesses worldwide. As a result, many states raised serious concerns about the security of their digital infrastructure and the vulnerability of their data to foreign spying. After these events, discussions on digital sovereignty became increasingly prevalent in both academic and policy circles. The strategic importance of digital sovereignty for preserving national autonomy in the digital era was highlighted, for instance, during consultations conducted by the **French National Digital Council** in 2014. Scholars and policymakers argued that the growing influence of major internet companies had created new forms of economic dependence, necessitating legislative solutions that balance the protection of national interests with the promotion of open and competitive digital markets[3].

The COVID-19 pandemic more recently brought these issues to the forefront. The crisis was described by many experts as a wake-up call, emphasizing the strategic importance of technological autonomy. Several European countries relied on Google's and Apple's digital infrastructures and application programming interfaces (APIs) to develop contact-tracing apps during the pandemic, highlighting the extent to which critical digital capabilities are concentrated within private platforms.

In recent years, European policy priorities have increasingly reflected the significance of digital sovereignty. For instance, the new **European Commission for the 2024–2029 period** includes a portfolio dedicated to **"Tech Sovereignty, Security, and Democracy,"** illustrating the

[1] Pierucci, « Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace », 2.
[2] Pierucci, « Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace », 2.
[3] Pierucci, « Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace », 2.

central role that technological control and digital autonomy now play in contemporary politics."[1]

- **Dimensions of digital sovereignty :**

Digital sovereignty comprises several interrelated dimensions: **data sovereignty, technological sovereignty, cybersecurity sovereignty, and legislative (or legal) sovereignty**.

Data sovereignty refers to the ability of a nation or region to exercise full control over the data collected, stored, and processed within its borders. This includes establishing legal and regulatory frameworks for data management and protection, as well as fostering a domestic data economy.

Technological sovereignty denotes the capacity of a nation or region to independently develop, maintain, and manage its own technology assets and infrastructure, including hardware, software, and network systems. This dimension is particularly critical for innovation and national security.

Cybersecurity sovereignty enables a state or region to defend its digital infrastructure and systems against cyber threats. It encompasses the implementation of cybersecurity standards and certifications, as well as the establishment of protocols for responding to cyber incidents.

Finally, **legislative sovereignty** refers to the authority of a nation or region to create and enforce its own legal regulations in the digital domain. This includes governing digital platforms, e-commerce, online services, and related digital activities.[2].

Although the terms **"digital sovereignty"** and **"cyber sovereignty"** are sometimes used interchangeably, they are not identical. Digital sovereignty encompasses a broader set of concerns, including data governance, technological autonomy, digital infrastructures, and platform regulation. In contrast, cyber sovereignty primarily focuses on governmental control over cyberspace and internet governance. In this sense, cyber sovereignty can be understood as a subset of the broader concept of digital sovereignty.

The suitability of traditional, state-centric conceptions of sovereignty is increasingly challenged by the transformations brought about by globalization in the digital era. While earlier stages of globalization reorganized political and economic interconnections, recent developments introduce a deeper shift: the emergence of computational infrastructures as the fundamental architecture through which power is organized and exercised.

In this context, **The Stack** model provides a critical framework for understanding how digital technologies are not merely instruments of governance but actively generate new forms of sovereignty. Bratton conceptualizes computation as governance itself, rather than merely a tool

[1] Federico Pierucci, "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace," Springer (2025): 3.
[2] Gábor Hulkó, Judit Kálmán, and András Lapsánszky, "The Politics of Digital Sovereignty and the European Union's Legislation: Navigating Crises," *Frontiers in Political Science* 7 (2025): 3.

for governance, arguing that technological systems constitute structural conditions that organize social and political order. [1].

According to Bratton, **The Stack** is a planetary-scale megastructure composed of interdependent layers, including Earth, Cloud, City, Address, Interface, and User, each of which represents distinct but related domains of governance and computation.

The **Earth** layer represents the physical and material foundations of computation: data centers, energy systems, and submarine cables. Sovereignty at this layer is exercised by states, energy providers, and telecommunication companies that own or control infrastructure critical for cross-border digital flows.

The **Cloud** layer, encompassing global computing networks and platforms, is dominated by private actors, including tech giants such as Google, Amazon, and Microsoft, whose control over cloud storage and processing power grants them considerable influence over global digital operations.

At the **City** layer, municipal governments and local service providers manage regional infrastructure, implementing smart-city technologies and local networks. The **Address**, **Interface**, and **User** layers involve standardization, protocol management, and access regulation, where NGOs, international standards bodies (e.g., Internet Corporation for Assigned Names and Numbers – ICANN; Institute of Electrical and Electronics Engineers – IEEE), and platform operators play crucial roles in shaping usage, advocating for digital rights, and influencing interoperability. By mapping actors onto each layer, digital sovereignty is revealed as multi-actor and multi-layered, extending beyond states to include private corporations, civil society, and international organizations.

Crucially, this structure is an emergent construction resulting from the interaction of various technological, economic, and political processes rather than from a single design or centralized authority.

The Stack, an **"accidental megastructure,"** evolves as a result of platformization and infrastructure growth, influencing global systems while simultaneously being shaped by them [2]. This layered architecture introduces a vertical model of power, in which different forms of authority are distributed across multiple levels that operate simultaneously rather than within a single, territorially bounded framework.[3].

The infrastructures supporting digital systems are firmly anchored in territorial and physical structures, far from immaterial. What is generally referred to as the **"Cloud"** depends on a vast network of underwater cables, data centers, and energy-intensive logistical systems that enable data to be stored and circulated on a global scale. This material dimension demonstrates that digital sovereignty must be understood through the governance of the physical infrastructures supporting international data flows, rather than being reduced to issues of software, platforms, or regulation alone.

[1] Bratton, *The Stack on software and sovereignty*, 18.
[2] Bratton, *The Stack*, 5,6.
[3] Bratton, *The Stack*, 68.

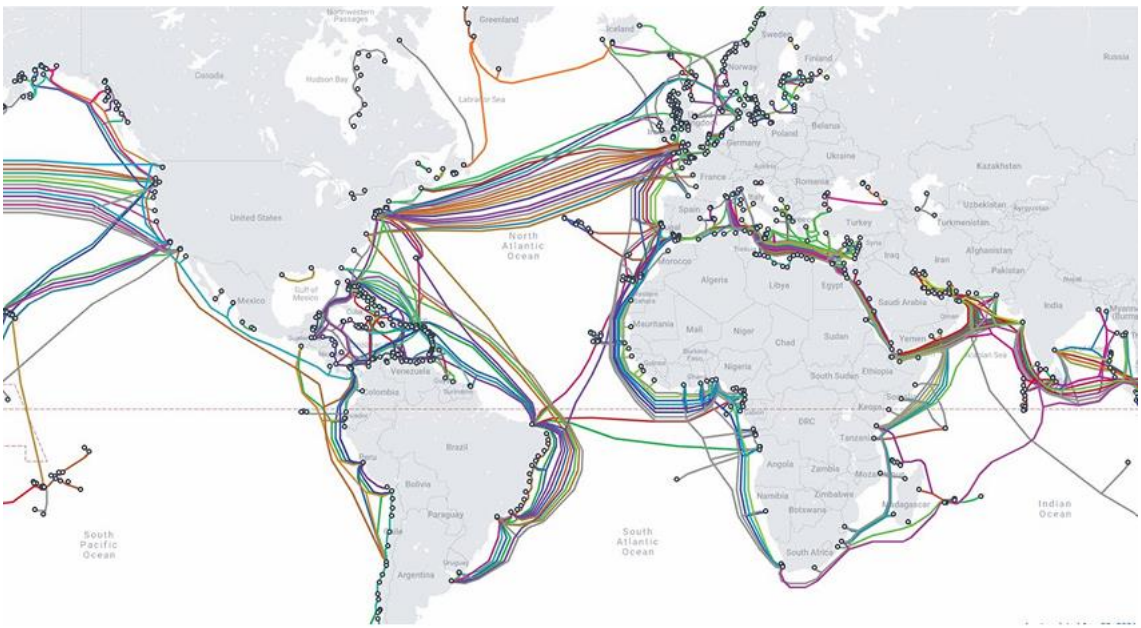
In this way, the ability to organize, safeguard, and manage these infrastructures—which serve as the base upon which higher levels of computational authority are constructed—is inextricably linked to the exercise of power in the digital era. This corresponds to what Bratton conceptualizes as the **Earth layer** of The Stack, which foregrounds the material and energetic conditions of computation and highlights the dependence of digital sovereignty on territorial and infrastructural foundations. [1] . This development gives rise to what is known as **"infrastructural sovereignty,"** where authority stems from the capacity to direct and shape the technological layers that constitute digital existence. As a result, sovereignty is increasingly exercised through the management of infrastructures, data flows, and computational systems rather than being solely associated with physical control. Authority is thus dispersed among multiple entities, each functioning at a different level of The Stack, including states, corporations, and transnational networks.

This layered computational architecture reconfigures sovereignty in a way that transforms the landscape of geopolitical struggle rather than eliminating it. The ability to influence and shape various layers of The Stack—from digital platforms to physical infrastructures—is increasingly a determinant of power. This shift forms the foundation for understanding the evolving rivalry among great powers, which will be explored in the next chapter by analyzing contests over digital platforms, infrastructures, and data governance.

Because there is no pre-existing spatial framework in which entities and their relationships reside, traditional concepts of **territories** and **borders** are hardly applicable in the cyberspace of digital sovereignty. In this space, information (data) flows through nodes connected by edges, and the entities and their relationships constitute the "space" itself. Consequently, rather than being defined by physical dimensions, cyberspace is dynamically configured by the connections and interactions among its constituent parts. The following maps will illustrate (a) the submarine cable structure and (b) the development of cross-border data flows to highlight this important feature[2]

Figure 1 : submarine cables

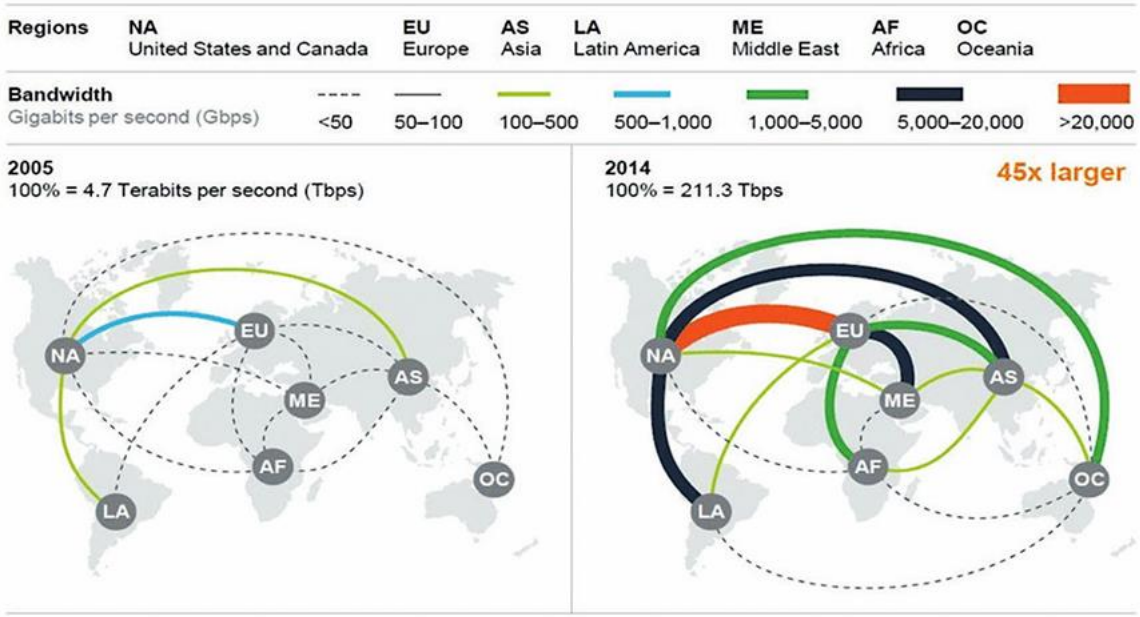
[1] Bratton, *The Stack*, 76.
[2] Federico Pierucci, "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace," published online April 22, 2025 :11



Source : Adapted from Federico Pierucci, "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace," based on Ganz et al., 2024

The map shows the structure of the submarine cables, more than 99% of global Internet traffic is transmitted through undersea fiber-optic cables. Unlike physical borders, these cables cut across multiple jurisdictions and pass by international waters, owned by private corporations and foreign governments, which challenge the state's sovereignty and create dependency by undermining national autonomy over critical infrastructures.

Figure 2 : Changes in global data flow between regions



Source: Adapted from Federico Pierucci, "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace," based on McKinsey Global Institute. (2016 de facto March) de facto in (Sarafanov & Shuqiang, 2017)

The second map represents changes in global data flows between regions, in the years 2005 and 2014.

In 2005, the total global bandwidth was only 4.7 Terabits per second (Tbps). By 2014, it reached 211.3 Tbps—a 45x increase in just nine years. The thickest lines (highest bandwidth) are between North America (NA) and European Union (EU), and increasingly between North America and Asia.

Within less than a decade, the bandwidth becomes increasingly larger, heavily concentrated between North America and Europe, which reflects the sharp increase in data flows with the dominance of Western economic in digital infrastructures and the fact that most major platforms and cloud services were headquartered in the United States.

The map also marks that some regions are dependent on external actors, for instance the absence of a line between Africa and Latin America, shows that not all regions participate equally in the global data flows, raising questions of justice, equality,and inclusion in the global digital order .

By 2014, the data flows increased between Asia and the rest of the world, reflecting the rise of Asian power,as producers and consumers of digital services. This marks the transition to multipolar digital order.

This comparison reveals that sovereignty in cyberspace is not static but evolves with economic power, technological capacity and geopolitical shifts. the transition from 2005 to 2014 represents not just a quantitative increase in data, but a qualitative shift in power.

The majority of international internet traffic is transported over vast underwater fiber-optic networks via submarine cables, which form the backbone of global digital connectivity. Because of their complex ownership arrangements and multinational layouts, these infrastructures present significant challenges to digital sovereignty despite their crucial function. National control over data transmission is limited because these cables traverse multiple jurisdictions and often extend into international waters, making it impossible for a single state to fully regulate or secure them.

The concentration of ownership in the hands of foreign entities and private companies further reinforces this limitation by creating dependencies that constrain states' control over critical communication infrastructure. Additionally, these networks are vulnerable to geopolitical threats that directly affect data security and the continuity of digital services, ranging from interception to sabotage. In this context, data—often referred to as the "new oil"[1]—becomes a strategic resource at the center of modern power hierarchies. Control over the movement of data is a key aspect of digital sovereignty, as the rapid growth of cross-border data flows has increased its economic and political significance. According to *The Stack: On Software and Sovereignty*, authority is increasingly exercised not only through physical control but also via the capacity to regulate the flows and infrastructures that constitute the global digital environment.

- **Can a State Claim Full Control over Digital Sovereignty ?**

Despite being home to most of the world's major technology corporations, the United States faces the same dilemma of sovereignty in the digital sphere[2]. The debate here is whether a country that dominates software and platforms can truly claim digital sovereignty if it lacks control over the material foundations of technology, notably semiconductors and the production of chips, concentrated particularly in Taiwan.

The Taiwan China tension has therefore pushed both US and the EU to invest in semiconductor manufacturing and critical raw materials, in order to reduce reliance on external suppliers[3].

Besides Sovereignty is being challenged by the rise of private actors, the war in Ukraine for instance reveals this vulnerability, when Elon Musk restricted Starlink services in Crimea, raising concerns in Washington; should national security hinge on the decisions of private entrepreneurs, or must the state reclaim authority over infrastructures critical to military and political objectives?[4] These examples show how the absence of essential resources, geopolitical tensions, and the risk of relying on private actors pose obstacles to the achievement of an absolute digital sovereignty.

[1] F. Pierucci. "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace." *Digital Society*, 4 (2025),12

[2]Federico Pierucci, *Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace*, received January 17, 2025, accepted March 26, 2025, published online April 22, 2025 , 3.

[3] Pierucci, *Sovereignty in the Digital Era,3.*

[4] Pierucci, *Sovereignty in the Digital Era* , 3.

Moreover, in a world ruled by power and interests,the legal protections of sovereignty are no longer absolute,although UN Charter focused on collective security,the world is shifting towards a "law of the strongest",US forces kidnapping the Venzuelian President Nicolas Maduro for is a clear evidence in this context[1].If International law can't protect a president, can it really protect a state's digital data?

Unilateral state control is practically difficult because of the transnational nature of digital interactions and data flows, yet some states impose rules on data localization, which refers to the process by which data is stored and processed inside a country's borders, which gives governments stronger national control over information flows, because they can enforce their own laws directly on the servers and infrastructure located within their territory[2].

However, this practice can also fragment the global Internet, instead of an interconnected network where data moves freely across borders, localization rules isolate global Internet.Consequently this localization strengthens national control but erodes the idea of borderless internet[3].

In the context of global standards and norms, internationally cannot be negotiated beyond any single state's control. Even private corporations like Google, Meta and Microsoft participate in the process of norms settings, in addition, data stored on servers outside national territory erodes full control over digital sovereignty[4].

1.3.Theoretical Perspectives in International Relations

1.3.1.Digital Sovereignty Through the Lenses of IR Theories:

The debate over digital sovereignty begins at the physical layer of the stack, made of mines,cables and chips.From a Classical Realist perspective, this is a struggle driven by the will to power, the idea that states naturally compete to dominate their rivals to survive the anarchy of the international system,and secure national interests. Rooted in Hans Morgenthau's writings, **Classical Realism** emphasizes the pursuit of power as a central motivator of state behavior[5], Morgenthau listed elements of national power such as natural resources and industrial capacity[6]. In the digital age, this ontology of power can be updated to include data and digital infrastructures, cloud services, fiber-optic cables, and semiconductors, as the new strategic resources. Just as oil shaped geopolitics, dependence on foreign data centers or semiconductor supply chains now shapes digital sovereignty. For instance, Europe's reliance

[1] Jan Muhammad Shaikh, "Maduro's Capture: How The U.S. Redefined Power, Oil, And Sovereignty In Latin America," The Friday Times, January 5, 2026, https://www.thefridaytimes.com/05-Jan-2026/u-s-seizes-nicol-s-maduro-daring-operation-triggering-regional-global-fallout.
[2] Kaya, M., and Hamza Shahid. "Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance." *Interdisciplinary Studies in Society, Law, and Politics* (2025) 222,225.
[3] Kaya and Shahid, Cross-Border Data Flows and Digital Sovereignty , 220.
[4]Kaya and Shahid, *Cross-Border Data Flows and Digital Sovereignty*, 224.
[5] Morgenthau,Politics Among Nations , 4.15
[6] Morgenthau,Politics Among Nations , 80,86.

on U.S. cloud providers like Amazon Web Services (AWS) or Microsoft Azure exposes vulnerabilities akin to energy dependence on OPEC.

For instance, in May 2025 Microsoft services used by the International Criminal Court (ICC) were suddenly interrupted. This disruption was not a random technical glitch but a direct consequence of geopolitical pressure. The U.S. government, through executive sanctions, targeted the ICC after it issued arrest warrants against Israeli officials. Because the ICC relies heavily on Microsoft's cloud services (email, file management, digital collaboration), the sanctions immediately translated into operational paralysis[1].Therefore, Digital infrastructures are not neutral, this example shows how dangerous is to be dependent on foreign digital infrastructure , by that political decisions can become technical disruptions, undermining the daily functioning of critical institutions, and exposing the international system to the duplicity of standards, biased system toward the powerful countries , ruled by weaponized supply chains.

Resource scarcity creates dependence on external actors, whether foreign governments or Big Tech firms. Yet Classical Realism, with its state-centric approach, ignores non-state actors such as GAFAM or ICANN, whose power in the digital realm rivals that of states. Digital sovereignty from a classical realist perspective can be primarily understood in terms of power and competition, as tool to secure national interest.However, it remains predominantly state-centric and does not adequately account for the role of non-state actors.

A structural Realist analysis reveals a more systemic pressure,because the international system is anarchic and states cannot be certain of other's intentions, they fall into a security dilemma[2], this is evident in the strategic competition over Taiwan's semiconductor industry, which functions a physical chokepoint in the global digital economy,if a state does not produce its own chips, it is considered structurally vulnerable. However, Structural Realism neglects norms, identities, and governance structures essential to understanding digital sovereignty.

The ability to leverage cyberspace to generate advantages and influence outcomes is what Joseph Nye refers to as **cyber power** [3].In the digital era, this distribution increasingly incorporates technological capabilities. Control over data flows, digital infrastructures, and technological innovation has therefore become a critical element of national power.

This materialistic view is challenged by a Constructivist shift in political identity. **Constructivism** argues that Identities and interests are not fixed or given by nature; they are socially constructed[4] through interaction and sustained by common meanings. This view highlights that concepts such as "anarchy" or "authority" are not inevitable features of world politics but contingent on how states interpret and enact their relationships.From a constructivist approach, authority is socially constructed too ,through shared beliefs and international recognition.When a private actor like Elon Musk has the power to dictate the communications of a nation via Starlink,the very identity of the state as the sole sovereign is reconstructed,

[1] *Whitepaper: Risks with US Cloud.* December 2025. https://cryptify.com/wp-content/uploads/2025/12/Whitepaper-Risks-with-US-cloud.pdf. , 1,2.
[2] Kenneth N. Waltz,Theory of International Politics , 187.
[3] Nye, *The Future of Power*, Online-Ausg (PublicAffairs, 2011), 123.
[4] Wendt, *Social Theory of International Politics,1*,2.

defining the authority by technical capacity rather than territorial borders.Moreover, Constructivism explain how the meaning of sovereignty is being redefined, border control, once a strictly sovereign function, is now partly outsourced to U.S. private companies called Hyperscalers : these firms ;Amazon Web Services,Microsoft Azure and Google Cloud Platform ,operate massive, interconnected data centers and provide services at scale (storage, AI, analytics, biometric processing)which are subject to U.S. jurisdiction, meaning European border data stored with them can be compelled into U.S. legal processes, transform border security into a digital market[1], where European policy decisions can be influenced by foreign commercial interests and legal constraints. Yet constructivism,risks underestimating the material infrastructures,semiconductors, cables, satellites that underpin sovereignty.

Liberalism argues that interdependence prevents war and overcome the security dilemma through trade and shared interests[2], The Kantian triangle ;institutions, trade, and democracy, reduces conflict, with interdependence serving as a driver of prosperity. The European Union's General Data Protection Regulation (GDPR) exemplifies institutional cooperation to harmonize digital governance[3]. Yet liberal ontology underestimates power asymmetries: not all states benefit equally from openness. The Global South, for instance, is exploited by tech giants through data extraction without equitable returns. Moreover, if cooperation is a win-win game, why do states pursue digital protectionism, such as India's data localization laws? [4]States turn to digital protectionism when the perceived benefits of cooperation clash with security, sovereignty and economic imperatives. In India, policymakers argue that localising data helps safeguard personal information, curtail foreign espionage and preserve national security, even as the broader digital market expands.

However **Neoliberal Institutionalism** acknowledges a more complicated reality: Complex Interdependence[5], which argues that in an increasingly interconnected world, states are legally and economically entwined that absolute digital sovereignty is far from being fully achieved.For instance, if a country tries to stay isolated from the global data hub to gain absolute control, it risks collapsing its own economy. From a Neoliberal perspective,states are rational actors who pursue absolute gains, in the digital realm, this means that a state's primary interest is to maximize the economic and technical benefits of global connectivity, however this rational pursuit is complicated by a Prisoner Dilemma: while mutual cooperation, such as open data flows and shared infrastructures ,the rational fear that shared infrastructures may be weaponized , for instance, U.S. sanctions cutting Huawei off from global semiconductor supply chains forces states to invest in "defensive sovereignty", Instead of weakening Huawei, such measures push the company to develop its own technologies and reduce dependence on U.S. firms[6] .

---

[1] Georgetown Journal of International Affairs**.** "A Tool for Security? Cloud Computing in Border Control." March 17, 2026. https://gjia.georgetown.edu/2026/03/17/a-tool-for-security-cloud-computing-in-border-control.
[2] Dunne et al., *International Relations Theories*: 95.
[3] Ceko, *THE GLOBAL ROLE AND IMPACT OF THE GENERAL DATA PROTECTION REGULATION (GDPR): AN INTERNATIONAL COMPARATIVE APPROACH*, 46.
[4] Sen et Chadha, *DATA LOCALIZATION: AN ISSUE IN THE CROSS-BORDER DIGITAL ECONOMY*, 1517.
[5] Dunne et al., *International Relations Theories*, 115,120.
[6] Douglas B. Fuller, *Cutting Off Our Nose to Spite Our Face: US Policy toward China in Key Semiconductor Industry Inputs, Capital Equipment, and Electronic Design Automation Tools* (Baltimore: Johns Hopkins University, SSRN Scholarly Paper, Social Science Research Network, September 29, 2020) , 7.

However Neoliberalism underestimates the persistence of power asymmetries and the extent to which dominant actors ;both states and corporations can shape or constrain cooperative arrangements.

In this networked world, states resort to internet governance and the set of norms and rules.According to the **Normative Theory**, International Relations cannot be comprehended without taking values and obligations into consideration.Thus, Normative theory is essential for assessing the legitimacy of global practices and imagining a just international order since these principles emphasise that international politics is about ethical commitments in addition to power and interests[1] .European Union for example,follows this normative approach by setting rules and acts like the GDPR and the AI acts that will be discussed in the next chapters.The debate here is whether the Rule of Law can truly govern a global system that is technically built and owned by foreign private actors. However, normative theory remains at the level of ideals focusing on what ought to be rather than what is[2].

Dependency theory provides a critical lens for understanding digital sovereignty by focusing on technological advantages accumulated during earlier industrial revolutions continue to shape global hierarchies in the fourth Industrial revolution. Factors such as domestic investment, intellectual property protection positively influence technology transfer, yet the benefits accrue unevenly depending on a country's level of skills and infrastructure. Studies show that low skill economies tend to receive only low-tech transfers, while highly skilled societies attract advanced technologies, reinforcing structural inequalities.

In the digital era, this dynamic translates into unequal access to AI, data centers, and computing capacity, which are prerequisites for exercising sovereignty in this age. A study by Cardoso's observation that financial and technological penetration by developed centers produces unbalanced structures, where peripheral states remain dependent on external firms and capital and center states maintain dominance[3];The current digital order is based on the same logic, the Global South provides the raw data and mineral wealth, while the North retains the algorithmic intelligence.For developing nations,the pursuit of digital sovereignty is an act of decolonization,states struggle to break dependency relations where national infrastructure is hosted on foreign clouds and governed by foreign interests. Scholars describe Big Tech’s extraction of personal and communal data as a new form of colonialism[4], akin to resource plunder. Yet it does not provide concrete policy tools for achieving sovereignty, leaving global south states struggling to translate critique into practice.

International Political Economy interprets digital sovereignty as part of the broader diffusion of power away from states towards markets,firms and transnational actors, Susan strange argues that sovereignty must be understood through the lens of structural power, which is defined as the ability to shape the frameworks of security, production,finance and knowledge.In the digital

[1] Dunne et al., *International Relations Theories*, 46,49.
[2] Yiyang Mei and Matthew Sag, *The Illusory Normativity of Rights-Based AI Regulation* (arXiv preprint, August 12, 2025),55.
[3] Ndzendze et Marwala, *Artificial Intelligence and International Relations Theories*, 105,109.
[4] Marcus Vinícius De Freitas, *Digital Sovereignty and Data Colonialism: Shaping a Just Digital Order for the Global South*, Policy Paper No. 38/25 (Rabat: Policy Center for the New South, October 2025) .

era, these structures appear in control over data flows, technological infrastructures and standards, Susan Strange argues that markets are more powerful than states in determining who gets what[1], extended to digital sovereignty, private corporations and supranational institutions increasingly dominate the cyberspace. Her analysis of the knowledge structure[2]shows how authority over information systems and technology reconfigurate sovereignty. Building on that, IPE interpretes digital sovereignty as contested and multilayered negotiation among states, firms and global institutions, rather than a purely state centric concept.

However, IPE's has limits when applied to digital sovereignty,Strange's framework was developed in the context of financial and trade structures,and does not fully anticipate the specific dynamics of artificial intelligence,algorithms, or platform power.Her structural approach tends to emphasize economic actors and market forces but struggles to account for political and normative dimensions of digital sovereignty.

Taken together, these theories provide complementary ontologies and epistemologies for analyzing digital sovereignty. Realism focuses on material infrastructures, Liberalism emphasizes institutions and interdependence,Neoliberalism focuses on complex interdependence ,Constructivism highlights norms and identities, Dependency theory,structural inequalities, and Normative theory raises ethical imperatives, and IPE reveals how structural power over finance,production, and knowledge shifts from states toward markets,firms, and transnational actors.Yet each framework has its limitations : Realism ignores non-state actors, Liberalism underestimates asymmetries, Constructivism neglects materiality, dependency theory lacks policy tools, and Normative theory remains abstract, and IPE was developed in the context of financial and trade structures and struggle to fully account for the specific dynamics of algorithmic governance, platform power, and artificial intelligence.

1.3.2.The Need for a New Hybrid Theoretical Framework :

Although both traditional and modern theories of international relations offer useful frameworks for understanding world politics, their capacity to explain digital sovereignty is more nuanced. Digital sovereignty, a concept at the intersection of technology, governance, and power, challenges conventional notions of territory, authority, and control, necessitating a multifaceted analytical approach. No single framework is sufficient to fully comprehend digital sovereignty. Each focuses on a particular dimension; power, interdependence, norms, legitimacy, or inequality,yet each also has significant limitations.What is needed therefore is not the abandonment of existing frameworks but their structured combination into a hybrid analytical approach adequate to explain the complexity of digital sovereignty.

[1] Strange, Susan. *The Retreat of the State: The Diffusion of Power in the World Economy.* Cambridge: Cambridge University Press, 1996, 4,5.
[2] Strange, *The Retreat of the State*, 121,125.

In building this hybrid framework, a foundational question must be answered:Who controls the structures through which digital sovereignty is exercised or denied? **Susan Strange's concept of structural power**[1] provides the answer; in the digital era, structural power operates through four knowledge-based structures: control over information ,data flows, control over standard setting and control over AI systems, whoever controls these structures shapes the terms on which all other actors ;states, corporations, citizens, must operate.In this hybrid framework, International political economy is foundational because it explains why digital sovereignty is contested in the first place.States,firms and institutions compete over digital sovereignty because structural power over AI and data is the defining source of authority in the contemporary international system.

However, IPE cannot explain why states respond differently to the same structural pressures, why some inequalities persist even when states have formal sovereignty, or how norms and identities shape sovereignty claims.

Realism, answers how does the claim over digital sovereignty reshapes the balance of power between states, and why do states treat digital infrastructure as a strategic sovereignty indicator?

Relying on **Ndzendze and Marwala**, the distribution of AI capabilities among states is becoming the primary determinant of strategic positioning, in addition to military and economic power[2]. A state's digital sovereignty is therefore directly proportional to its position in this **AI balance of power**[3].

Also, when applying the concept of **security dilemma** logic to digital infrastructure, a state that depends on foreign AI systems, cloud providers, or semi-conductor supply chains is structurally vulnerable regardless of its formal sovereignty status.

In this context, powerful states use technological dependency as a coercive instrument such as sanctions,and infrastructure exclusion, making them new tools in the geopolitical competition, this process is a kind **of weaponnized interdependence**.For instance, the Huawei ban US semiconductor export controls against China[4], show how effective the realistic approach in explaining this phenomenon.However, as mentioned above,Realism ignores the role of private corporations as sovereign actors.

Furethermore, Structural inequality is best interpreted through dependency theory, which provides the economic and structural mechanism, explaining the technological gaps between the center and periphery, which clarify why digital sovereignty means something fundamentally different for a state like Rwanda or Senegal than it does for France or United States, for the former ones, digital sovereignty is about reducing dependency, as for the latter ones it is about maintaining dominance.

[1] Susan Strange,States and Markets,2nd ed. London: Pinter Publishers,1994, 23,25.
[2] Ndzendze et Marwala, *Artificial Intelligence and International Relations Theories*, 69.
[3] Ndzendze et Marwala, *Artificial Intelligence and International Relations Theories*, 66.
[4] Fuller, *CUTTING OFF OUR NOSE TO SPITE OUR FACE*, 7.

According to Constructivism, sovereignty is a social construction, each state perceive behavior in cyberspace and digital governance depending on the norms, identities, and their proper understanding of reality.This explains why United States, China and the EU defend digital sovereignty with different strategies ,that will be discussed in the next chapter.

Drawing on **Ndzendze and Marwala's** , after studying IR theories they found out that there's two exisiting patterns ,traditional theories which retain stronger predictive power at the interstate level and explaining state behavior , while critical theories offer deeper explanatory value for sub-state and structural dynamics which understanding help societies, norms meanings and historical backgrounds. This framework operates across four level of analysis; global structures, interstate competition, asymmetric relations,and normative constestation[1].

Overall, this hybrid framework operates across four distinct levels of analysis. At the global structures level, IPE, which is a core theory in this model, explains how structural power over AI, data, and standards defines authority in the International system. At the interstate competition level, realism shows how digital sovereignty reshapes the balance of power and how states treat digital infrastructure as a strategic indicator. At the asymmetric relations level, dependency theory highlights structural inequalities between center and periphery, clarifying why sovereignty means reducing dependency for weaker states but maintaining dominance for stronger ones. Finally, at the normative contestation level, Constructivism explains how norms, identities, and perceptions shape sovereignty claims, together these four levels demonstrate that no single theory is sufficient, but their structured combination provides a hybrid analytical approach capable of explaining the complexity of digital sovereignty.

Summary of Chapter One:

[1] Ndzendze et Marwala, *Artificial Intelligence and International Relations Theories*, 161,162.

This chapter has demonstrated how the concept of sovereignty has evolved in response to globalization and the digital revolution. While sovereignty has historically been grounded in governmental authority and territorial control, it now encompasses new domains, particularly the digital sphere, where concerns about data, technology, and infrastructure have become central. Analysis of key theoretical approaches in international relations reveals that, although traditional frameworks remain useful, they are insufficient to account for these changes, necessitating a structured combination of these theories to cover digital sovereignty in four dimensions:Global structure, interstate level,asymmetric relations and finally normative level.

In this context, digital sovereignty should be understood as a reconfiguration of traditional sovereignty rather than its replacement. The following chapter, which examines how artificial intelligence reshapes power dynamics and the exercise of sovereignty in contemporary international politics, is built upon this conceptual and theoretical foundation.

PART TWO : Artificial Intelligence and the Reconfiguration of Sovereignty

2. Artificial Intelligence as a Geopolitical and Infrastructural Transformation

2.1. Artificial Intelligence as a New structure of Power

This section constitutes the core of the analysis, addressing how AI challenges and reconfigures states' digital sovereignty. It examines AI as a transformative force that redistributes authority from states to technological actors, erodes territorial foundations, and deepens structural inequalities, thereby creating new forms of digital dependency.

2.1.1. The Development of Technology and Artificial Intelligence

The trajectory of technological change can be understood through the framework of the four Industrial Revolutions (4IR). The Fourth Industrial Revolution, as defined by Klaus Schwab represents an "abrupt and radical change"in technological development[1].

The First Industrial Revolution began in England between 1760 and 1840, driven by the invention of the steam engine and the expansion of railroads, which mechanized production and transformed agrarian economies into industrial ones. The Second Industrial Revolution, spanning from the 1870s to the early 1900s, was characterized by the widespread use of electricity, the development of assembly lines, and the rise of mass production. This period also witnessed major innovations such as the telegraph, the telephone, and advances in the steel industry.

The Third Industrial Revolution, occurring from the 1960s to the 1990s, is commonly referred to as the digital or computer revolution. It was marked by the development of semiconductors, mainframe computers, personal computers (from the 1970s to the 1980s), and the emergence of the Internet in the 1990s, as discussed in Chapter One.

The Fourth Industrial Revolution, which began in the early 2000s and continues to the present, builds upon the digital revolution and is characterized by the proliferation of advanced technologies such as artificial intelligence, big data, and interconnected digital systems, AI powered by Machine Learning, Internet of things, robotics and biotechnology .[2] reshaping governance, sovereignty and geopolitics.

[1]Marwala, Tshilidzi. *Artificial Intelligence and Emerging Technologies in International Relations.* London: World Scientific, 2020 ,33.
[2] Marwala, Tshilidzi. *Artificial Intelligence and Emerging Technologies in International Relations.* London: World Scientific, 2020, 32,35.

These technological mutations have consistently reshaped politics,economies and societies, culminating today in the rise of modern Artificial Intelligence as a core element of the fourth Industrial Revolution.

The development of artificial intelligence can be traced back to early philosophical and mathematical foundations, particularly the logic of deductive reasoning introduced by Aristotle. Subsequent contributions by thinkers such as Leibniz, Babbage, and Hollerith further paved the way for the emergence of AI by advancing formal logic, computation, and data processing[1].

In this context, Al-Khwarizmi made a decisive contribution to the development of algorithms. His work in arithmetic and algebra laid the foundations for systematic approaches to calculation, which remain central to modern computational systems[2].

A major milestone in the evolution of artificial intelligence was Alan Turing's 1950 proposal of the Turing Test for machine intelligence. This framework explored the possibility of machines imitating human cognitive processes and introduced the idea that machines could learn, a concept he described as a "child program."[3].

The mid-twentieth century marked the institutional birth of AI, particularly with John McCarthy's coining of the term "artificial intelligence" in 1956 and the establishment of dedicated research laboratories at MIT and Stanford University. However, early optimism was followed by periods of stagnation due to technological limitations and overinflated expectations, leading to cycles of reduced funding known as "AI winters."

The first AI winter (1966–1980) was characterized by critical assessments such as the ALPAC Report in the United States and the Lighthill Report in the United Kingdom, both of which highlighted the limited progress in machine translation and general AI research. These critiques resulted in significant funding cuts and declining confidence in the field. The period ended with renewed interest driven by commercial successes, notably the creation of the expert system XCON (R1) by Digital Equipment Corporation.

The second AI winter (1987–1990) followed the collapse of the expert systems market. Specialized Lisp machines were replaced by more cost-effective alternatives, leading to a market downturn and the withdrawal of both corporate and governmental support, particularly in the United States and Japan.

The recovery of AI began in the 2000s, supported by advances in computational power, data availability, and algorithmic innovation. Breakthroughs such as Google's voice recognition

[1] Yevstratov Yurii Ihorovych, "The History of Artificial Intelligence," Visnyk of Science and Education no. 8 (38) (2025): 912–922, 915.
[2] P.M.A. Aleeshan, M.N.P. Rifasha, and Mohamed Haniffa Mohamed Nairoos, "The Contribution of Medieval Muslims to the Development of Modern Science: A Review of Al Khwarizmi," *International Journal of Social Science and Economic Research* 8, no. 2 (February 2023): 219 .
[3] Yevstratov, « THE HISTORY OF ARTIFICIAL INTELLIGENCE DEVELOPMENT », 917.

technologies in 2008 and DeepMind's AlphaGo victory in 2016 demonstrated the growing capabilities of AI systems, surpassing human performance in complex tasks.

Today, modern AI systems, driven by machine learning techniques, are capable of performing a wide range of sophisticated tasks. As noted by D. Pchelyansky and S. Voinova, these include pattern recognition, situational analysis, logical reasoning, understanding new information, learning and self-learning, and strategic planning[1].

2.1.2. Conceptualizing Artificial Intelligence as a Transformative Power:

Kate Crawford argues that artificial intelligence (AI), or more precisely machine learning, is neither "artificial" nor "intelligent," but rather a set of political and social practices that both reflect and reproduce existing social structures. In this sense, AI constitutes a form of power leveraged to serve the interests of dominant actors, relying on training data, human expertise, natural resources, and physical infrastructures[2].

To understand why AI should be considered political rather than merely technical, three fundamental questions arise: what is being optimized, for whom, and who gets to decide?[3] Accordingly, AI should be understood as a material, social, and political infrastructure. Crawford proposes a topographical model composed of multiple scales to map AI, describing it as an extractive industry that depends on energy, labor, and data.[4]

The High-Level Expert Group on Artificial Intelligence defines AI as a set of human-made software and hardware systems designed to pursue complex goals. These systems operate in both physical and digital environments through a sequence of processes: perceiving their environment through data collection, interpreting this data, reasoning upon it, and ultimately making rational decisions based on predefined objectives [5] .

Scholars approach AI from multiple perspectives. The technical approach conceptualizes AI as a set of computational tools, focusing on algorithms and their functionality. In contrast, the sociological approach views algorithms as products of human interaction among programmers and designers, reflecting cognitive biases and cultural contexts, thus emphasizing that AI is never neutral. The legal approach considers AI as part of regulatory and normative frameworks, while the philosophical approach examines the ethical implications of AI decision-making and questions its legitimacy[6].

[1] Yevstratov, « THE HISTORY OF ARTIFICIAL INTELLIGENCE DEVELOPMENT », 918,919.
[2] Crawford, *Atlas of AI*, 8,9.
[3] Crawford, *Atlas of AI*, 9.
[4] Crawford, *Atlas of AI*, 15.
[5] Nizov, Vladimir A. *The Artificial Intelligence Influence on Structure of Power: Long-Term Transformation. Legal Issues in the Digital Age* 6, no. 2 (2025): 183–212: 187.
[6] Nizov, *Artificial Intelligence Influence on Structure of Power*, 185.

From an operational perspective, AI consists of algorithm-based systems capable of autonomous action through machine learning (ML). These systems identify behavioral and cognitive patterns by processing large volumes of data. Machine learning typically involves several stages: data collection, storage, preparation, algorithm training, and application development. This process includes acquiring raw data, storing it in data centers, formatting and labeling it, and ultimately deploying predictive models in applications such as mobile software, medical diagnostics, military operations, geospatial analysis, and autonomous vehicles[1].

Operationally, AI can thus be defined as a set of human-made software and hardware systems that, through machine learning processes, can autonomously recognize, interpret, and act upon data to achieve complex objectives. Beyond its technical dimension, however, AI also constitutes a material, political, and social infrastructure. It relies on energy, data, and human labor, and has the capacity to shape social structures, serve dominant interests, and transform the nature of governance, authority, and sovereignty, thereby necessitating the development of legal and ethical frameworks.

Related concepts:

The Internet of Things (IoT) refers to interconnected devices that communicate through data exchange, creating a physical–digital interface across domains such as smart cities, energy systems, and surveillance infrastructures [2].

5G connectivity: refers to a fast telecommunications technology, reaching 100 gigabits per second, through network slicing; process whereby 5G hubs are installed nearly to users, offering a faster connection. Geopolitically, this technology is dominated by China and USA, each rival seeks to develop its own strategy, which makes 5G a Geopolitical issue rather than a technical revolution [3].

Semiconductors: are materials with electrical conductivity between that of conductors and insulators. They are employed in the manufacture of various electronic devices, including diodes, transistors, and integrated circuits. Such devices have found widespread application due to their compactness, reliability, power efficiency, and low cost[4].

Graphic processing unit GPU: A Graphics Processing Unit (GPU) is an electronic circuit designed to perform a large number of mathematical calculations rapidly. Originally developed to accelerate 3D graphics rendering, GPUs have, since their introduction in the 1990s, been increasingly used beyond computer graphics in areas such as high-performance computing and machine learning [5].

[1] Marwala, Tshilidzi. *Artificial Intelligence and Emerging Technologies in International Relations.* London: World Scientific, 2020, 6.
[2] Marwala, *Artificial Intelligence and Emerging Technologies*,, 7.
[3] Marwala, *Artificial Intelligence and Emerging Technologies*,, 8.
[4] « Semiconductor | Definition, Examples, Types, Uses, Materials, Devices, & Facts | Britannica ».
[5] « Graphics Processing Unit (GPU) | Definition, Applications, History, & Facts | Britannica ».

Machine Learning: a discipline of AI that provides computers with the ability to learn without being explicitly programmed. It focuses on the development of algorithms that can analyze data, make predictions or decisions based on new inputs [1].

Cloud computing: it refers to both applications delivered as services over the internet and the hardware and systems software in the datacenters that provide those services. The datacenter hardware and software is what we call a cloud [2].

Artificial intelligence is therefore not a neutral technology. When applied in sectors such as education, healthcare, or judicial systems, it can reproduce and even amplify structural inequalities in ways that benefit dominant states, institutions, and corporations. AI can thus be understood as a form of power rooted in economic and political structures, aimed at maximizing profit and consolidating centralized authority[3]. Understanding AI as power requires moving beyond its technical dimensions and examining the material and political conditions from which it emerges, as well as the hierarchies it reinforces.

AI, in this sense, constitutes an extractive form of political power, rooted in the salt lakes of Bolivia and the mineral mines of the Congo, and constructed from datasets labeled by crowdworkers who classify human actions, emotions, and identities. It is used to guide drones over Yemen, direct immigration enforcement in the United States, and adjust credit scores that assess human value and risk across the world [4].

In this regard, AI does not only reflect existing power relations; rather, it deepens them and transforms fundamental notions such as authority, sovereignty, and territorial control, as will be further explored.

2.1.3.Data as a New Raw Material

While Part One examined data flows as a challenge to territorial sovereignty in the digital age, this section approaches data from a different angle—not as information crossing borders, but as the core resource from which artificial intelligence derives its power, and through which structural authority is accumulated by those who control it.

Just as oil powered industrial capitalism, data powers algorithmic capitalism. Without data, there would be no AI, no algorithms, and no redistribution of power. Crucially, the more data an AI system possesses, the more powerful it becomes. Data has therefore emerged as a strategic resource. This transformation is not only technological but also deeply political, as it raises a

[1] « Machine learning | Data Science, Algorithms & Automation | Britannica ».
[2] Michael Armbrust et al., "A View of Cloud Computing," *Communications of the ACM* 53, no. 4 (April 2010): 50–58, 50.
[3] Crawford, *Atlas of AI*, 211.
[4] Crawford, Atlas of AI, 218.

fundamental question: who owns data, and what does that ownership imply for sovereign authority?

The answer reflects a transformation in the nature of power through what scholars describe as "assetization"—the process by which data is legally and economically constructed as a form of capitalized private property[1],Through this process, corporations have effectively placed the primary resource of AI power beyond the reach of traditional state regulation. In this context, data is not merely collected; it is propertized, making sovereign claims over it structurally difficult to maintain.

Between 1950 and 2020, American corporations—particularly the GAFAM constellation (Google, Apple, Amazon, and Microsoft)—shifted from reliance on physical assets to the accumulation of intangible assets. Big Tech firms have thus transformed data into a highly valuable economic resource, with user data at the core of their strategic power[2],with user data as a core strategic resource.

Consequently, data—and therefore AI capability—is increasingly owned and controlled by private actors whose authority over this "new oil" in many cases surpasses that of sovereign states.

In this context, Shoshana Zuboff defines "surveillance capitalism" as an economic order that transforms human experience into raw material ready to be extracted, analyzed, predicted, and sold. This process operates through several stages. First, corporations collect what Zuboff terms "behavioral surplus"—data generated by human activity online that exceeds what is technically necessary to improve services and is therefore available for alternative uses. This surplus is not incidental; rather, everyday activities such as purchases and social interactions are systematically captured to generate behavioral data aimed at prediction and profit maximization.

This behavioral surplus feeds into what Zuboff describes as "behavioral futures markets," in which predictions about future human behavior are sold to companies seeking to influence consumer decisions, political opinions, and social choices.

This predictive capacity evolves into what Zuboff terms "instrumentarianism," a new form of power that does not merely observe and predict human behavior but actively seeks to modify it through the architecture of digital environments. Unlike industrial power, which automated machines, instrumentarian power automates human behavior by shaping choices and engineering actions at a scale that exceeds traditional state sovereignty.

This process—from data extraction to behavioral modification—poses a fundamental challenge to sovereignty. Due to its invisible and borderless nature, private corporations acquire the

[1] Daniel Neyland, Véra Ehrenstein, and Sveta Milyaeva, "Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech," *Big Data & Society* 8, no. 2 (July–December 2021): 1–12, 3.
[2] Neyland, Ehrenstein, and Milyaeva, *"Data as Asset?,7*.

capacity to predict and influence the behavior of citizens through recommendation algorithms, targeted content, and personalized interfaces, thereby operating beyond the effective reach of state authority[1] .

Artificial intelligence is fundamentally built upon an extractive logic shaped by continuous data accumulation. As Vannevar Bush observed, machines possess "enormous appetites," and the data they consume shapes how they interpret the world. This dynamic is particularly significant for dominant powers such as the United States and China, for whom data collection becomes an act of structuring global hierarchies[2].

In this sense, control over data is increasingly transformed into a form of sovereign power, concentrating authority over human behavior in the hands of private actors.

2.2. The reconfiguration of digital sovereignty in the AI era

While the previous section conceptualized AI as a structure of power, this section examines the implications of this shift for digital sovereignty. It analyzes the mechanisms through which AI erodes, fragments, and reconfigures state control over the digital domain, including data, infrastructure, platforms, and algorithmic systems.

2.2.1. Erosion of territorial sovereignty

The principle of Westphalian sovereignty rests on a foundational assumption: that the state holds exclusive authority within its territory, free from external interference. In practice, however, this principle has been selectively applied and frequently violated, particularly by great powers through coercion and consent, thereby challenging both Westphalian and legal sovereignty[3]. The AI era introduces a qualitatively new form of violation—one that operates through invisible and cross-border data flows. These flows challenge traditional notions of sovereignty and jurisdiction. Maintaining control over data within national boundaries becomes increasingly difficult due to its dynamic and transnational nature. As a result, legal systems grounded in territorial containment struggle to regulate data effectively, raising fundamental questions about how authority, control, and rights should be exercised in the digital age.

What makes data particularly resistant to sovereign control is its intrinsic properties. Data is highly mobile, crossing borders in fractions of a second without the awareness of users or the consent of states. It is also divisible, capable of being copied, partitioned, and stored

[1] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019), 14.
[2] Crawford, *Atlas of AI*, 121.
[3] Krasner, *Sovereignty* organized hypocrisy7.

simultaneously across multiple jurisdictions. These characteristics make it impossible to anchor data within a single territorial space, resulting in what can be described as location independence—a condition in which data becomes detached from the physical infrastructure on which it is stored. This creates a structural disconnect between territorial law and digital space[1].Together these features mean that sovereign assumption of territorial containment –a term that refers to the ability of the state to govern its borders is inadequate in the AI era. [2]. Together, these features render the traditional sovereign assumption of territorial containment—the ability of the state to govern within clearly defined borders—increasingly inadequate in the AI era.

These properties of data, do not exist in a vaccum, they are made possible by a specific infrastructure, which is **cloud computing** systems , that determine These properties of data do not exist in a vacuum; they are enabled by specific technological infrastructures, most notably cloud computing systems. Cloud infrastructure determines where data is stored, who can access it, and under which sovereign authority it is governed. Despite its seemingly immaterial and borderless nature, cloud infrastructure is deeply physical, built from rare earth minerals, lithium, crude oil, and brine, and located in specific geographical areas. As Kate Crawford argues, "the cloud is the backbone of the artificial intelligence industry, and it is made of rocks, lithium brine, and crude oil"[3].

The majority of global cloud infrastructure is controlled by a small number of American corporations—Amazon Web Services, Microsoft Azure, and Google Cloud—whose servers are geographically distributed yet remain subject to U.S. jurisdiction. This creates a fundamental sovereignty dilemma: when a state or its citizens store data on foreign infrastructure, that data becomes subject to external legal frameworks.

The U.S. CLOUD Act (2018) exemplifies this jurisdictional expansion, requiring American providers to comply with law enforcement requests even when data is stored abroad, thereby extending U.S. jurisdiction beyond its territory. In contrast, the European Union's General Data Protection Regulation (GDPR) adopts a human-centric approach, imposing strict rules on personal data transfers to protect individual rights. The tension between these frameworks is illustrated by the Schrems II ruling (2020), in which Maximilian Schrems successfully challenged Facebook Ireland's data transfer practices. The Court of Justice of the European Union invalidated the EU–U.S. Privacy Shield, citing insufficient protection of EU citizens' data under U.S. surveillance laws. This decision forced companies to rely on alternative mechanisms, such as Standard Contractual Clauses (SCCs), which remain complex and legally uncertain[4].

[1] Jennifer Daskal, *"The Un-Territoriality of Data," Yale Law Journal* 125, no. 2 (2015): 326–398 ,366 , 397.

[2] Jennifer Daskal, *"The Un-Territoriality of Data," Yale Law Journal* 125, no. 2 (2015): 326–398 ,366 , 397.

[3] Crawford, *Atlas of AI*, 31.

[4] Taiwo Justice Olorunlana, *Securing the Global Cloud: Addressing Data Sovereignty, Cross-Border Compliance, and Emerging Threats in a Decentralized World*, *International Journal of Science, Architecture, Technology, and Environment* 2, no. 5 (May 2025): 1394–1407,1397.

This jurisdictional conflict reveals a fundamental transformation in sovereignty in the AI era: while states retain the capacity to legislate, they increasingly lack the ability to contain data. The interaction between data flows, cloud infrastructure, and competing legal regimes ultimately challenges the classical assumption of territorially bounded sovereign control.

2.2.2. The Redistribution of Authority Between States and Corporations in the AI Era

Studying the implications of artificial intelligence for digital sovereignty raises several core questions: through which mechanisms is AI implemented? Can states maintain sovereignty over AI? Conversely, can states use AI to enhance their digital sovereignty? And can these two dynamics coexist?

Drawing on Srivastava and Bullock's taxonomy, states exercise power through AI across multiple dimensions[1]:

One key dimension is instrumental power, whereby AI enhances direct state control. For instance, in the military domain, autonomous weapons systems can reduce human involvement in the exercise of violence. In the economic domain, states use AI to strengthen governance capacities; AI systems can analyze large datasets to detect tax evasion and fraudulent activities. A concrete example is the use of AI in Medicare programs in the United States to identify healthcare fraud. In such cases, AI reinforces digital sovereignty by enabling the state to exert greater control over economic flows and social programs through technological means. However, these benefits are unevenly distributed, as many Global South states lack the necessary technological and infrastructural capacity.

In the financial sector, AI is not only used for fraud detection or tax enforcement but also for macroeconomic governance. AI models can forecast inflation trends and recommend interest rate adjustments, thereby supporting state decision-making processes. In this context, AI enhances sovereign competence by improving the state's ability to govern effectively through data-driven insights.

However, this empowerment is accompanied by a structural tension. Many of these AI systems are developed and controlled by private corporations or foreign actors, placing states in a position of dependency. As a result, while AI may strengthen state capacity in practice, it can simultaneously undermine autonomy, creating a paradox at the heart of digital sovereignty[2].

In terms of structural power, AI enables dominant states to shape the environment within which other actors operate. For instance, the United States reinforces its leadership in AI by controlling access to critical resources, such as advanced semiconductors, and by restricting China's access to these technologies, thereby limiting its capacity to compete. This dynamic reflects what

[1]Swati Srivastava and Justin Bullock, *"AI, Global Governance, and Digital Sovereignty"* , 5.
[2] Srivastava and Bullock, *"AI, Global Governance, and Digital Sovereignty."*, 5.

Henry Farrell and Abraham Newman describe as "weaponized interdependence." In this sense, sovereignty extends beyond the domestic regulation of AI uses to include the ability to shape global dependencies through control over key infrastructures.

Third, discursive power refers to the ways in which states use AI to shape interests, ideologies, and identities. For example, by delegating the distribution of benefits to AI systems, states may reinforce neoliberal logics of efficiency and privatization. This, in turn, influences how citizens perceive governance and the role of the state[1].

By integrating AI across structural, discursive, and instrumental domains, governments can consolidate their sovereignty and strengthen their position within the international system. The debate, therefore, is not limited to regulating AI, but extends to how states can strategically deploy it to reinforce authority. However, this process simultaneously generates new forms of inequality, which will be further examined.

In sum, states are not merely passive recipients of AI-driven transformations; rather, they actively leverage AI to consolidate power. Yet, this consolidation is uneven, as it primarily benefits technologically advanced states, while excluding weaker states from fully participating in or shaping this emerging order.

States increasingly leverage the perceived threat of corporate power as a justification to reassert sovereign control[2], for example by imposing stricter regulations, nationalizing infrastructure, and investing in the public sector in order to regain control over data centers, communication networks, and AI platforms.

However, states are not the only governing actors. Platforms such as Google, Facebook, Amazon, and Apple do not merely provide services; they organize, regulate, and monetize human interactions at a scale that resembles—and in some respects surpasses—traditional state functions. They establish rules governing everyday interactions, control information flows, resolve disputes between users, and accumulate behavioral data as a source of structural power.

In doing so, these platforms acquire what Benjamin Bratton describes as a quasi-sovereign status, governing digital spaces with an authority that operates parallel to that of the state[3].Moreover, corporations exercise discursive power by normalizing surveillance capitalism and shaping citizens' perceptions of data rights and privacy in ways that serve corporate interests [4].

Sovereignty in the digital age is not a zero-sum game between states and corporations; rather, it is being reconfigured. States remain sovereign, but their authority is increasingly expressed through hybrid arrangements that embed private actors within sovereign practices. This results

[1] Srivastava et Bullock, « AI, Global Governance, and Digital Sovereignty », 2.
[2] Srivastava et Bullock, « AI, Global Governance, and Digital Sovereignty », 10.
[3] Bratton, *The Stack*, 42.
[4] Zuboff, *The Age of Surveillance Capitalism,16*.

in what can be described as hybrid sovereignty—a dual exercise of authority shared between states and corporations. In this sense, states are not necessarily weakened by collaboration with private actors; instead, sovereignty itself is transformed to incorporate both public and private sources of power, particularly in the governance of AI and digital infrastructures.

Such collaborations are increasingly visible in everyday contexts, including smart cities, airports, and surveillance systems such as Amazon Ring cameras integrated into policing networks. These examples illustrate that sovereignty is not exercised in opposition to private interests, but often through cooperation, reinforcing its hybrid character[1].

As AI systems continue to evolve, a more advanced form—autonomous AI—has emerged, capable of operating without direct human intervention. [2]. This development raises critical concerns, as the governing agent itself may become partially ungovernable, posing significant ethical and political challenges.

The war in Ukraine provides a concrete illustration of this transformation. Non-state actors, particularly major technology corporations, have become decisive participants in conflict dynamics. Microsoft and Amazon provided Ukraine with critical cloud infrastructure, enabling the relocation of government data and ensuring continuity across ministries, schools, hospitals, and financial institutions. Their support extended beyond data storage to include threat intelligence, helping counter hundreds of cyber intrusions. Meanwhile, Palantir Technologies contributed advanced analytical tools for processing satellite and battlefield data, assisting military operations and the documentation of war crimes.

These developments demonstrate that digital sovereignty in wartime is shaped not only by interstate rivalry but also by dependence on private corporations, whose infrastructures, policies, and leadership decisions can directly influence the escalation or de-escalation of conflicts.

A fourth key actor is SpaceX's Starlink, which has become a critical backbone of battlefield communications. According to its CEO, Elon Musk, the company's support to Ukraine has reached approximately $80 million. However, access to this infrastructure has at times been shaped by Musk's personal decisions, highlighting the discretionary power exercised by private actors.

The company restricted the use of its satellite services on several notable occasions. First, in late 2022, Ukrainian forces reported that coverage was unavailable in occupied territories they were attempting to liberate, including Kherson, Zaporizhzhia, Kharkiv, Donetsk, and Luhansk. Furthermore, Musk refused to activate Starlink coverage along the Crimean coast, preventing Ukraine from deploying drone submarines against the Russian fleet in Sevastopol, arguing that such actions could escalate the conflict. Similarly, in February 2023, Starlink imposed

[1] Srivastava et Bullock, « AI, Global Governance, and Digital Sovereignty », 12.
[2] Srivastava et Bullock, « AI, Global Governance, and Digital Sovereignty », 7.

additional restrictions by limiting the use of its technology for offensive operations, including drone strikes[1].

Susan Strange anticipated this dynamic in her theory of structural power, noting that technological change would push states to form alliances not only with other governments but increasingly with corporations[2]. Ukraine's reliance on Microsoft, Amazon, Palantir, and especially SpaceX's Starlink confirms this argument: technology firms have become autonomous actors whose infrastructures are essential to state survival, yet whose interests and decisions may diverge from those of the states they support. This tension between dependency and autonomy highlights how digital sovereignty is contested not only between great powers, but also between states and the corporations that control critical nodes of the global digital order.

The exercise of power in the AI era is therefore no longer a state monopoly; rather, it is contested, layered, and shared among public authorities, private corporations, and algorithmic systems, which risk exceeding direct human control as their autonomy increases. The central question, then, is what this reconfiguration means in practice for digital sovereignty. The following section addresses this question.

2.2.3. Digital sovereignty Reconfigured: Authority, Accountabiliy and Democratic issues

The transformations examined in the previous sections—the erosion of territorial control, the emergence of contested spaces between states and corporations, and the rise of autonomous AI systems—do not merely challenge digital sovereignty; they reconfigure it from within. As a result, new features of sovereignty are emerging in the AI era:

The hybrid sovereignty[3] concept, the erosion of democratic accountability and the emergence of a structural gap between where power is exercised and where citizens can meaningfully contest it[4].

The first impact is **the transformation of sovereign authority**. The classical concept of sovereignty was built exclusively on states, hybrid sovereignty replaces this model with one where sovereign power is shared by states and private actors through AI infrastructures[5],This transformation is not only practical but also conceptual. Sovereign decisions concerning surveillance, welfare distribution, and information governance are increasingly made through

[1] Broeders et al., « Digital corporate autonomy », 1196,1198.
[2] Broeders et al., « Digital corporate autonomy », 1197.
[3] Srivastava et Bullock, « AI, Global Governance, and Digital Sovereignty », 12.
[4] Pasquale, *The Black Box Society*, 215.
[5] Srivastava et Bullock, « AI, Global Governance, and Digital Sovereignty », 12.

systems owned and operated by unelected and unaccountable actors. As a result, the very nature of sovereignty is undergoing a fundamental shift.

For example, in India, the state asserts sovereign control over AI while simultaneously depending on privately owned infrastructure developed by corporations. This illustrates the growing tension between formal sovereignty and infrastructural dependence[1].

Another significant impact of AI on digital sovereignty is the erosion of democratic accountability. Democratic systems are based on the assumption that citizens can elect decision-makers and hold them accountable through transparency and participation[2]. However, algorithmic governance systematically undermines this principle. When decisions are made by systems whose internal logic is opaque and legally protected as proprietary information, citizens are unable to contest them—a phenomenon often described as the "AI black box."[3]

Moreover, governments frequently lack the technical expertise required to effectively monitor the AI systems they deploy, as they depend heavily on private contractors whose advanced technologies often exceed public regulatory capacities. This dependency further weakens accountability mechanisms.

The accountability deficit becomes most acute when the state's legitimate monopoly on violence—a foundational attribute of sovereignty—is partially delegated to autonomous weapons systems capable of identifying and executing targets without direct human supervision.

More broadly, the power shift introduced by AI creates a democratic gap: authority increasingly resides in platforms that govern interactions and in algorithms whose accountability is oriented toward shareholders rather than citizens. Meanwhile, traditional mechanisms of democratic accountability[4]. such as elections, parliaments, courts, and constitutions—remain largely state-centric and struggle to adapt to these transformations.

In this context, democratic regimes face a fundamental challenge: states are exercising authority through automated systems that remain largely invisible to the citizens they are meant to serve.

Therefore, taken these factors together It can be assumed that AI impacts digital sovereignty first by **introducing a conceptual change**, which is **the hybrid authority, eroding accountability and creating a democratic gap**, which reveal that the reconfiguration of digital sovereignty is a structural transformation that changes classical sovereignty frameworks, and challenges democratic norms.

[1] Srivastava et Bullock, « AI, Global Governance, and Digital Sovereignty », 3.
[2] Nizov, « The Artificial Intelligence Influence on Structure of Power », 2025, 200.
[3] A. Buruiană, *"Black Box AI and the Sovereignty of Personal Data: Between GDPR and Digital Ethics,"* *European Journal of Law and Public Administration* 12, no. 1 (2025): 89–97, 90.
[4] Srivastava et Bullock, « AI, Global Governance, and Digital Sovereignty », 12.

The next section will examine how AI deepens global power asymmetries, producing new forms of dependency.

2.3.Global Power Asymmetries and Digital Dependency

The global digital order is defined by intense technological rivalries. Power is concentrated among a few dominant states—primarily the US and China—and the tech giants controlling critical infrastructure, chokepoint technologies, and innovation ecosystems. However, these rivalries exist within a broader framework of structural dependency: most nations rely heavily on foreign technology, creating systemic asymmetries that dictate their autonomy and vulnerabilities.

2.3.1. Technological Rivalries between U.S and China

As AI becomes a strategic asset, its development and control are concentrated among a small number of states and corporations. This concentration fuels geopolitical tensions and rivalries among dominant powers, leads to the weaponization of technological dependency as a coercive instrument, and results in the progressive marginalization of states that lack these capabilities. Understanding these rivalries is essential for understanding why the meaning of digital sovereignty changes depending on a state's positioning in the international system.

The Dimensions of Rivalry- A Comparative Overview :

The AI Index Report highlights the intensifying rivalry between the United States and China. Accordingly, the competition has evolved from a race over private funding and technical benchmarks into a struggle for dominance across the global AI stage in several dimensions.

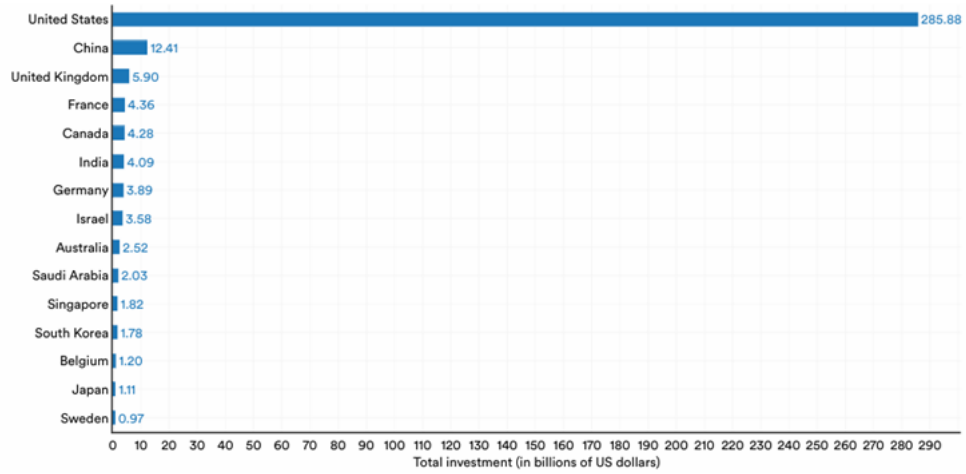
Starting with the scale of AI investment concentration, U.S. private AI investment grew to $285.9 billion in 2025—more than 23 times China's $12.4 billion[1]. In terms of AI models, however, the performance gap between the U.S. and China has effectively closed. In February 2025, DeepSeek-R1 briefly matched the top U.S. model, and by March 2026, the leading U.S. model held a lead of just 2.7%, a remarkably small gap compared to earlier years[2]

[1]Stanford Institute for Human-Centered Artificial Intelligence, *AI Index Report 2026* (Stanford, CA: Stanford University , 10.
[2] Stanford HAI, AI Index Report, 9.

In terms of compute infrastructure, US continue to dominate with hosting over 5400 AI data centers compared to China's 499, however both countries remain strategically dependent on Taiwan's TSMC for advanced chip fabrication, which shows a vulnerability in hardware sovereignty[1].

In terms of knowledge production, China leads in the sheer volume of AI publications, citations, and patents, whereas the U.S. retains primacy in high-impact patents and the number of globally recognized models, according to the 2026 AI Index Report.

Figure 3: Global private investment in AI by geographic area,2025

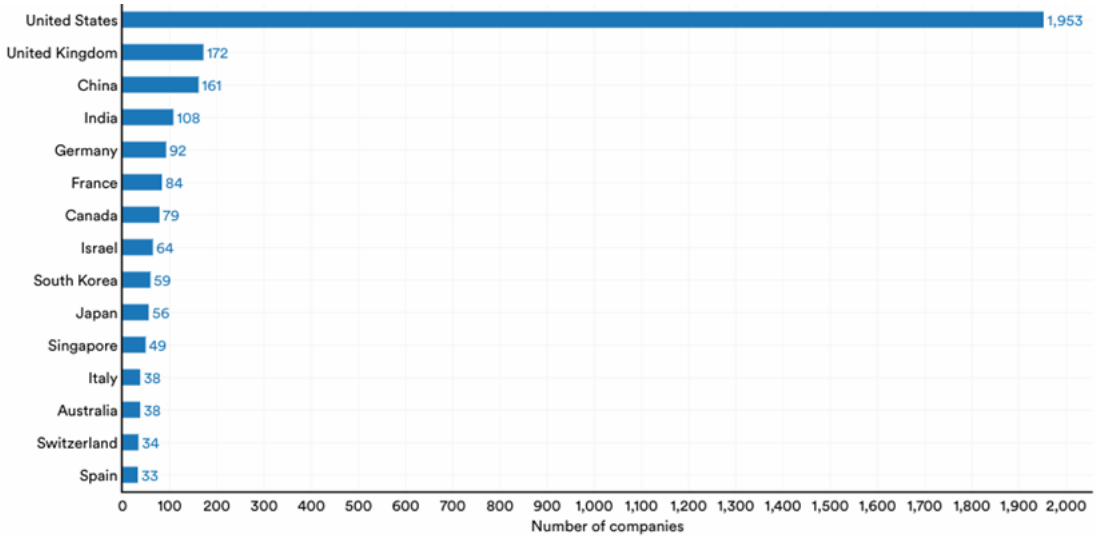


Source : Stanford Institute for Human-Centered Artificial Intelligence. *AI Index Report 2026*. Stanford University, 2026.

The chart points out the dominance of the United States in global private AI investment, with a significant gap comparing to China and other countries. Despite China's strong position, this imbalance reveals the concentration of technological power and the asymmetries in AI development.

Figure 4 : Number of newly funded AI companies by geographic area,2025

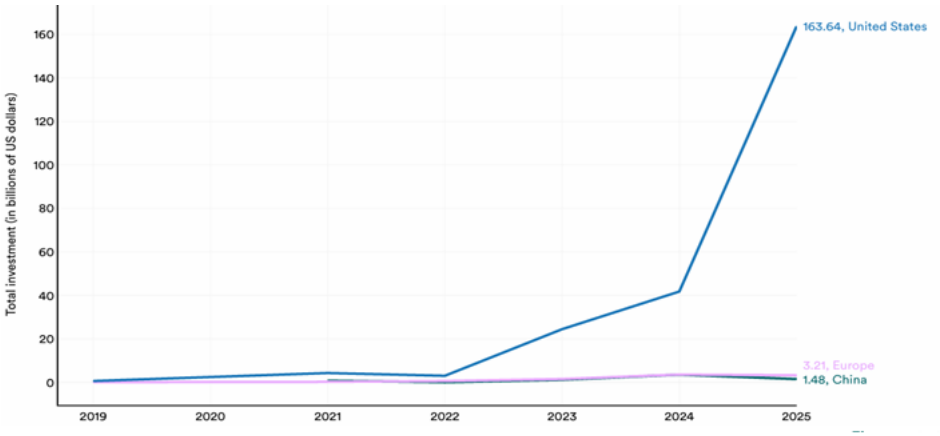
[1] Stanford HAI, AI Index Report ,32.



Source : Stanford Institute for Human-Centered Artificial Intelligence. *AI Index Report 2026*. Stanford University, 2026.

The distribution of newly funded AI companies reveals a strong concentration in the US, which far surpasses all other countries. While China, India, and several European states demonstrate growing activity, the gap remains vast. This counts as a structural advantage of the US innovation ecosystem.

Figure 5 : Global private investment in generative AI by geographic area,2019-25



Source : Stanford Institute for Human-Centered Artificial Intelligence. *AI Index Report 2026*. Stanford University, 2026.

Private investment in generative AI has increased after 2023, largely driven by the US, outpacing other rivals. This reflects the central role of private AI industry, in contrast to China and Europe which remain comparatively limited in private investment.

However, while the U.S. appears to be far ahead of China in private investment at first glance, China channels massive amounts of capital into AI through **state-backed** funds that do not

appear in private venture capital statistics. Between 2000 and 2023, these government funds invested approximately $912 billion across various industries, with $184 billion allocated specifically to AI companies.[1].

China has declared to become the world's leading AI power by 2030. In **2017,** it launched **China's Next Generation Artificial Intelligence Development Plan** which represents a state-led strategy to position the country as a global leader in artificial intelligence by 2030. The Plan integrates economic modernisation, social governance and military innovation, backed by massive state funding with the involvement of national corporations such as Baidu, Alibaba and Tencent[2].

However, the U.S has responded by moving toward securing its domestic AI supply chains and restricting China's access to the critical technological inputs that seek to slower the Chinese AI development pace. US responded with **the CHIPS Act**, as a strategic industrial policy, where it funds domestic semiconductor production, workforce training, while restricting China's access to semiconductors[3].

This AI race depends on highly concentrated chokepoints :the advanced semiconductors required to train AI models are produced by a small number of firms, with Taiwan Semiconductor Manufaturing Company TSMC, alone responsible for the majority of the world's most advanced chips[4].Whoever controls access to these chokepoints leads the race. The U.S tries to control through restrictions, sanctions, alliance, pressure on European and Middle Eastern partners to exclude China from critical supply chains, the Huawei ban is an evidence in this logic.

U.S is following a strategy to counter China's technological rise, first it **restricts the outflow of technology**, preventing American companies from exporting critical components or software to Chinese firms.

Second, it blocks the inflow of Chinese technologies through banning Chinese companies from building 5G networks in the U.S.

[1] Stanford Institute for Human-Centered Artificial Intelligence. *AI Index Report 2026*. Stanford University, 2026. https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf, 184.
[2]State Council of the People's Republic of China, *New Generation Artificial Intelligence Development Plan (2017)*, trans. DigiChina, Stanford University, July 20, 2017, https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017. .
[3]*The rise of techno-geopolitical uncertainty: Implications of the United States CHIPS and Science Act*, *Journal of International Business Policy* (2023), disponible sur PubMed Central, https://pmc.ncbi.nlm.nih.gov/articles/PMC10066984/pdf/41267_2023_Article_620.pdf. .
[4]Henry Farrell et Abraham L. Newman, "Cross-Network Weaponization in the Semiconductor Supply Chain," *International Studies Quarterly* 68, no. 1 (2024): 10.

Third, it applies a form of human decoupling, limiting the entry of Chinese scientists and students. And finally, it imposes sanctions in response to alleged cyberespionage by Chinese actors[1].

These measures reveal that US is trying to weaken China's technological capabilities in order to reinforce its dominance. It can also be concluded from this race that digital sovereignty is not only about protecting data or infrastructures, it has become a geopolitical contest where controlling flows of technology, people and networks define who is the dominant actor.

The United States Strategy:

The United States exercises digital sovereignty through weaponized interdependence—exploiting its asymmetric control over global technology networks to coerce rivals and preserve dominance. By commanding critical chokepoints, the U.S. effectively dictates how foreign actors, especially China, interact with the global AI ecosystem.

This strategy relies heavily on semiconductor containment. Through sweeping Department of Commerce export controls enacted in 2022 and 2023, the U.S. cut off China's access to cutting-edge AI hardware (like Nvidia's A100 and H100 processors) and the tools required to manufacture next-generation silicon. Domestically, Washington fences off its own infrastructure by banning or restricting Chinese platforms like Huawei and TikTok.

Because the semiconductor supply chain is highly specialized, this containment strategy requires strict allied alignment. The U.S. actively leverages its geopolitical leverage to pressure key partner nations—such as the Netherlands, which dominates lithography via ASML, and Japan, which controls essential chemical materials—into unifying behind its technology blockade[2].

China’s Strategy :

China's strategy relies on its **"dual circulation" policy**, designed to strengthen its technological independence and reduce vulnerability to foreign pressures. At its core, the policy emphasizes indigenous innovation and the urgent need to secure control over critical chokepoint technologies that could be weaponized against the country. This strategy operates across two main dimensions:

First, it focuses on building robust domestic supply and demand, turning the Chinese market into a self-sustaining engine of growth to achieve digital self-sufficiency. Second, it maintains selective global integration through initiatives like the Belt and Road Initiative (BRI), which

[1] Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford: Oxford University Press, 2023), 214.

[2] David Sacks,Emily Benson *Balancing the Ledger: Export controls on U.S Chip Technology to China, Center for Strategic and International Studies, October 2024, CSIS Analysis*[Balancing the Ledger: Export Controls on U.S. Chip Technology to China](#) .

project Chinese technological standards abroad, encourage domestic firms to invest internationally, and expand Beijing's geopolitical influence[1].

The ongoing U.S.–China tech war is pushing the world toward a new era of technological nationalism. As both countries close their markets to foreign technologies and invest heavily in domestic industries, competition shifts away from pure innovation toward structural protectionism. This shift fundamentally erodes the principles of open trade and global cooperation. The COVID-19 pandemic accelerated these trends by exposing critical vulnerabilities in global supply chains; this exposure pushed countries to adopt more nationalist industrial policies by limiting foreign investment, restricting exports, and incentivizing localized production.[2].

The trajectory of the U.S.–China digital rivalry illustrates how cyberspace has shifted from a struggle over market access to a global contest for infrastructural dominance. In the early 2000s, American firms such as Google, Yahoo, and Microsoft attempted to penetrate the Chinese market but were constrained by censorship and regulatory barriers. Google's eventual withdrawal in 2010 symbolized the limits of Silicon Valley's ambitions. These restrictions, reinforced by the Great Firewall, allowed China to foster its own domestic champions—Baidu, Alibaba, Tencent, and JD. By the 2010s, these firms not only controlled the domestic digital economy but also began expanding abroad, a move later accelerated by initiatives like the Digital Silk Road launched in 2015.

Consequently, U.S. policymakers abandoned hopes of opening China's market and shifted toward containing Chinese tech firms globally. This was notably demonstrated by the Clean Network Initiative in 2020, which pressured states and companies to exclude Chinese hardware and applications from their digital stacks. This policy reflected a broader strategic pivot: rather than merely competing within China, Washington aimed to prevent hybrid tech stacks that combined Chinese hardware with American software, thereby forcing third-party countries to choose an alliance. Simultaneously, both governments began to instrumentalize domestic platforms as tools of statecraft. In the U.S., firms like Amazon and Google were integrated into national security collaborations, while in China, platforms like Alibaba and Tencent were subordinated to the party-state through military-civil fusion and disciplined when they resisted. Although these tech platforms retain agency, their centrality to global data flows ensures they remain pivotal instruments in both Washington's and Beijing's grand strategies [3].

Chinese President Xi Jinping has emphasized that technological innovation now represents the decisive battleground of global competition, warning that the struggle for technological dominance will continue to intensify. In line with this vision, Beijing's latest Five-Year Plan sets measurable targets, deadlines, and accountability mechanisms for provincial and local

[1] Bradford, *Digital Empires*, 235.
[2] Bradford, *Digital Empires*, 242,243.
[3] Sebastian Schindler et al., *The Second Cold War: US–China Competition for Centrality in Infrastructure, Digital, Production, and Finance Networks, Geopolitics,* August 28, 2023,1098,1100.

governments, with the explicit aim of strengthening indigenous capabilities, reducing reliance on foreign technologies, and advancing emerging fields.

On the American side, Eric Schmidt, former CEO of Google, has cautioned that many in the United States underestimate China's progress. He argues that China is closing the gap in critical domains and could, by the 2030s, surpass the U.S. in economic scale, research investment, scientific output, tech deployment, and computing infrastructure.

To assess this trajectory, the Belfer Center report reviews two decades of progress across key technologies. It concludes that China has become a "full-spectrum peer competitor" in artificial intelligence. Furthermore, Beijing has gained a first-mover advantage in 5G, overtaken the U.S. in quantum communication while narrowing the lead in quantum computing, and is actively challenging American dominance in semiconductors, biotechnology, and green energy supply chains. Although the U.S. continues to lead in semiconductor design, biotechnology, and innovation networks, China's comprehensive mobilization—which integrates talent development, research investment, and state policy—has weakened America's long-standing status as the sole science and technology hegemon [1].

Towards a Digital Thucydides Trap?

The U.S.–China tech war is unlikely to produce a single winner or a unipolar tech superpower; instead, both countries are advancing in distinct domains. China leads in smartphone sales, telecommunications equipment, social media platforms like TikTok, and **the electric vehicle (EV) ecosystem**, including lithium-ion batteries. Conversely, the U.S. retains its dominance in advanced semiconductor design, mobile gaming, and foundational software ecosystems. Analysts warn that this fierce competition could escalate into a broader geopolitical confrontation, potentially triggering a Thucydides Trap—which occurs when a rising power threatens to displace an established hegemon. Taiwan's central role in advanced semiconductor manufacturing further intensifies these anxieties. Even if a direct military conflict is averted, economic decoupling is expected to persist as both sides increasingly restrict exports, block cross-border investments, and maximize domestic tech capabilities[2].

2.3.2. Structural Inequalities and Digital Dependency

Colonial logics never truly disappeared; instead, they have extended into the digital age. The same historical pattern is repeating itself through the "four-X" formula of colonialism: **explore, expand, exploit, and exterminate**. Big Tech explicitly applies this process within the digital sphere. Platforms *explore* the personal details of individuals, *expand* into intimate personal

[1]Graham Allison, Kevin Klyman, Karina Barbesino, and Hugo Yen, *The Great Tech Rivalry: China vs. the U.S.*, Avoiding Great Power War Project (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, December 2021) , 3,6.
[2] Bradford, *Digital Empires*, 246,251.

spaces and workplaces, *exploit* behavioral data, and *exterminate* alternative ways of organizing social life by imposing corporate standards[1].

What is striking about this paradigm is that society itself has become the new territory. Human social interactions, political debates, and daily activities have been transformed into profitable assets—a dynamic conceptualized as **data colonialism[2]**. On a macro level, this shift does not merely affect individuals; it actively reshapes the international system. States that lack control over digital infrastructure, platforms, and computational capacity become structurally dependent on foreign technological centers—primarily the United States and China, which hold monopolies over cloud infrastructure, AI capabilities, and platform governance. This creates a new form of digital dependency, where state sovereignty is severely constrained by whoever controls global data flows.

A clear example of this dynamic is Facebook's "Free Basics" initiative. Launched under the guise of humanitarian digital aid to regions with weaker digital infrastructure—such as Colombia, Pakistan, Ghana, Kenya, Mexico, and the Philippines—the project ultimately reinforced structural dependency on a foreign corporation. In reality, Free Basics only allowed access to a highly curated, limited set of websites chosen by Facebook. Users could not browse the open internet, yet Facebook collected data on all of their activities, transforming "free access" into a mechanism for capturing new audiences and monetizing their information. In India, digital rights activists successfully argued that Free Basics was a form of digital colonialism, prompting the government to ban the service in 2016[3], This regulatory pushback underscores how colonial logics persist in the modern era, operating through entirely new technological mechanisms.

Can digital dependency be measured?

This thesis relies on **The Digital Dependence Index**, developed by **Maximilian Mayer and Yen-Chi Lu** in their 2022 working paper: Digital Autonomy? *Measuring the global Digital Dependence Structure*. The index was designed to capture how much a country relies on foreign digital technologies and infrastructures? and how vulnerable is it in terms of digital autonomy?

It is based on the following definition of **digital dependence**: " the extent to which actors in a particular country have to rely on foreign controlled digital technologies to perform digital activities". It compares data from 23 leading countries including the United States, China, Germany, India, Japan, South Korea, Brazil and South Africa, based on three dimensions:

- **The trade dependence**, which indicate the reliance on imports of information and communications technology, ICT goods and services

[1] Ulises A. Mejias and Nick Couldry, *Data Grab: The New Colonialism of Big Tech and How to Fight Back* (London: Pluto Press, 2020), 4.
[2] Mejias et Couldry, *Data Grab*, 61.
[3] Nick Couldry and Ulises Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford: Stanford University Press, 2019), 97.

- **Infrastructure dependence**; measures the reliance on foreign owned platforms, cloud services and digital ecosystems
- **Intellectual property (IP)dependence**, which shows reliance on patents and proprietary technologies concentrated in a few jurisdictions[1].

The DDI consists of three sub-indexes and 23 indicators:

Table 1. Composition of Digital Dependence Index DDI

Subindex A (Hardware)		**Subindex B (Software)**		**Subindex C (Intellectual property)**
Indicator I: Trade in ICT goods	**Indicator II: Information-Infrastructure**	**Indicator III: Trade in ICT services**	**Indicator IV: Information Infrastructure**	**Indicator V: ICT related patents**
• Computers peripheral equipment • Communication equipment • Consumer electronic equipment • Electronic components • Miscellaneous	• Smartphone • Tablet	• Telecommunications services • Computer software • IT consulting , IT design, IT management and IT training Licenses to computer software	• Browser • Search engine • Desktop OS • Mobile OS • Social Media	• Audio-visual technology • Telecommunications • Digital communications • Basic communication processes • Computer technology • IT methods for management • semiconductors

Source: **Maximilian Mayer and Yen-Chi Lu, Digital Autonomy? Measuring the Global Digital Dependence Structure.**

Within **the Sub-index A Hardware**, the first indicator measures trade in ICT goods including computers peripheral equipment, communication equipment, electronic components. This indicator reflects dependence on the physical architecture of digital economy.

The second Hardware indicator focuses on information infrastructures such as smartphones and tablets, which are important as control over devices gives control over data and digital access.

Within **Sub- index B Software**, the third indicator measures trade in ICT services, including telecommunications services, computer software, IT consulting, IT design, IT management, training and software licensing. They are equally important because states may possess digital infrastructures physically while remaining dependent on foreign software services.

[1] Maximilian Mayer and Yen-Chi Lu, *Digital Autonomy? Measuring the Global Digital Dependence Structure*, SSRN Working Paper No. 4404826 (Bonn: Center for Advanced Security, Strategic and Integration Studies, 2022) ,5.

The fourth indicator focuses on information infrastructures, including browsers, search engines, desktop operating systems, mobile operating systems and social media.

Sub-index C Intellectual Property, contains the fifth indicator, ICT related patents, including Audio-visual technology, telecommunications technologies, semiconductors and computer technologies. In the AI era, patent concentration reinforces asymmetrical power relations by allowing a small number of states and corporations to dominate the production of strategic technologies.

Building on these indicators, It can be concluded that the DDI reinforces the logic developed through Bratton's concept of the Stack, sovereignty in the AI era is multilayered, and power-dependency relations are defined through the control of the different layers of the Stack rather than territorial authority.

During the COVID-19 pandemic, states realized that sovereignty was not just about borders or military capacity, but about who controls the infrastructure, platforms, and data flows that society needs during emergencies. According to the Digital Dependence Index (DDI), 87% of states worldwide are highly vulnerable to foreign digital technologies. The U.S. was found to be the least dependent with a low DDI score of 0.47, while most other countries scored between 0.8 and 0.99, indicating severe vulnerability. In contrast, China and South Korea successfully reduced their dependency through targeted industrial policies focusing on domestic innovation ecosystems, while Europe continued to fall behind compared to both the U.S. and China[1].

Table 2. Four degrees of digital dependence

Degrees	DDI value	Ratio between domestic demand and foreign supply of digital technologies
Absolute independence	DDI = 0	Autarky.
Low sensitivity	0 <DD ≤0.25	Autonomy very high. Domestic digital technology is in a dominant position.
High sensitivity	0.25 < DDI < 0.5	Domestic supply delivers majority of digital tech. Considerable level of resilience.
Low vulnerability	0.5 DDI ≤ 0.75	Global markets supply majority of digital tech.
High vulnerability	0.75 DDI < 1	Autonomy very low. Foreign digital technology is in a dominant position.
Absolute dependence	DDI = 1	Foreign digital technologies fully cover domestic demand.

Source : Maximilian Mayer and Yen-Chi Lu, Digital Autonomy? Measuring the Global Digital Dependence Structure.

The table above conceptualizes digital sovereignty through varying degrees of digital dependence, measured by the Digital Dependence Index (DDI). The DDI calculates the relationship between domestic technological demand and reliance on foreign digital supply. At

[1] Mayer et Lu, « Digital Autonomy? », 1.

one extreme, absolute independence (DDI=0) corresponds to digital autarky, where domestic infrastructure and technologies fully satisfy national demand. At the opposite extreme, absolute dependence (DDI=1) reflects a situation in which foreign technologies entirely dominate domestic digital ecosystems, leaving states structurally vulnerable to external political, economic, and technological pressures.

The intermediate categories reveal that digital sovereignty is not binary but exists across distinct thresholds of sensitivity and vulnerability. *Low sensitivity* describes systems where domestic digital technologies remain dominant and national autonomy is relatively high, even within a framework of global interdependence. *High sensitivity* reflects an increasing reliance on external technologies, although domestic capacity still provides significant resilience. By contrast, *low vulnerability* and especially *high vulnerability* indicate deep structural dependence on foreign infrastructure, cloud services, platforms, semiconductors, and computational systems, which severely reduces a state's capacity to exercise autonomous control over its digital environment. Therefore, digital dependency cannot be measured through a single indicator; instead, it must be approached through composite variables reflecting infrastructural, technological, financial, and computational asymmetries.

This shifting landscape undermines traditional legal assumptions that anchor state authority to physical territory, a model that fails when applied to data moving fluidly across borders. For countries in the Global South, sovereignty is challenged on two primary fronts: first, their legal authority over data stored abroad is routinely bypassed by the extraterritorial legal claims of the United States or Europe; second, their domestic infrastructure and economies are deeply dependent on platforms and cloud networks located within these dominant states. This asymmetry reproduces historical colonial hierarchies, wherein the resources of the periphery—notably behavioral data and the critical minerals powering the AI industry—are extracted to enrich the global center.

Key findings of part Two:

This part has demonstrated that artificial intelligence reconfigures digital sovereignty through mechanisms that are simultaneously material, institutional, and structural. This systemic reconfiguration has been evaluated across five core analytical indicators:

- **Jurisdictional Tensions:** Evidence demonstrates that while states can pass domestic legislation, they cannot easily contain cross-border data flows or blunt the extraterritorial reach of foreign legal authority over vital digital systems.

- **Fragmentation of Authority:** The divide between states, tech monopolies, and autonomous systems manifests through *instrumental, structural, and discursive power*. This is epitomized by the Ukraine Starlink crisis, which marks **hybrid sovereignty** as the modern operative condition of digital politics.

- Erosion of Democratic Accountability: Algorithms are increasingly insulated from civic and state oversight due to the technical opacity of the **AI Black Box problem**.

- Deepening Structural Dependency: As measured by the *Digital Dependence Index (DDI)*, a staggering 87% of the world's nation-states now exist in conditions of high vulnerability to foreign-controlled digital ecosystems.

- The U.S.–China Hegemonic Race: The tech war between Washington and Beijing represents a grand geopolitical struggle. AI has transformed into a proxy conflict over the capacity to dictate the rules of the future international digital order.

The pursuit of digital sovereignty is no longer an isolated technical challenge; it is a structural revolution altering the very nature of power in international relations.

The following chapter will examine the practical strategies states deploy to reclaim and assert their digital sovereignty.

PART THREE : Policy Responses and Practical Transformations

3. Digital Sovereignty in Practice: AI Governance and Strategic Responses

3.1. National, Regional and Global Responses: Asserting Digital Sovereignty From Within

3.1.1. National AI Strategies and Digital Sovereignty Models

By April 2024, over 94 countries have created their national artificial intelligence strategies NAS, which reflects the recognition on how AI has become a sovereign concern [1],this growing interests in AI resulted the need to implement an AI governance as a part of asserting digital sovereignty agenda.

The governance of AI was exclusive to private actors such as Big Tech firms, consequently, states and intergovernmental organisations balenced the situation by intervening to assert digital sovereignty, yet these interventions are partial and symbolic , which lead to a fragmented hybrid form of governance, where sovereignty claims coexist with market logics[2] .

- **Digital Sovereignty Models as a Framework for AI national Strategies:**

  Digital Sovereignty Models as a Framework for AI national Strategies:

Before examining individual national strategies, it is necessary to establish the analytical framework through which they will be evaluated, scholars distinguish four models of digital sovereignty :

The right based model, emphasizes the protection of fundamental rights and individual autonomy, with constraining corporate power through regulation, the European Union illustrates this approach through GDPR and the AI act.

The state-based model focuses on the fusion of public authority and corporate capacity, where states invest heavily in domestic infrastructures and asserts state sovereignty over corporations, China's AI strategy illustrates this model.

The centralisation model is marked by the strong state control and the exclusion of foreign or non-state actors, prioritising national security and territorial sovereign, for instance Russia and Iran strategies that will be later analysed. Finally**, the market oriented model** points ou the " laissez-faire" principle, and based on competition and self-regulation, the example of the United States with the silicon Valley illustrate the neoliberal approach, though recent national security concerns such as restrictions on Huawei reveal the backward of the pure market logic[3]. These

[1] Albous et al., *AI Governance in the GCC States: A Comparative Analysis of National AI Strategies*, 2390.
[2] Radu, « Steering the Governance of Artificial Intelligence », 180.
[3] Samuele Fratini, Emmie Hine, Claudio Novelli, Huw Roberts, and Luciano Floridi, “Digital Sovereignty: A

models are essential in answering who governs digital space,on whose terms and how this reflects on sovereignty ? To compare digital sovereignty models in value foundations and operational dimensions, this thesis relies on a set of indicators derived from the literature, including data control, cybersecurity, relations with corporations, digital rights, technological self-sufficiency, and territorialization of cyberspace. As shown in the table each model is associated with specific **value codes**, refering to the different ideologies, and **descriptive codes** indicating concrete policy practices, to show why and how states act in each model.

X : indicates inclusion.

Table 3 : Construction of Models from codes

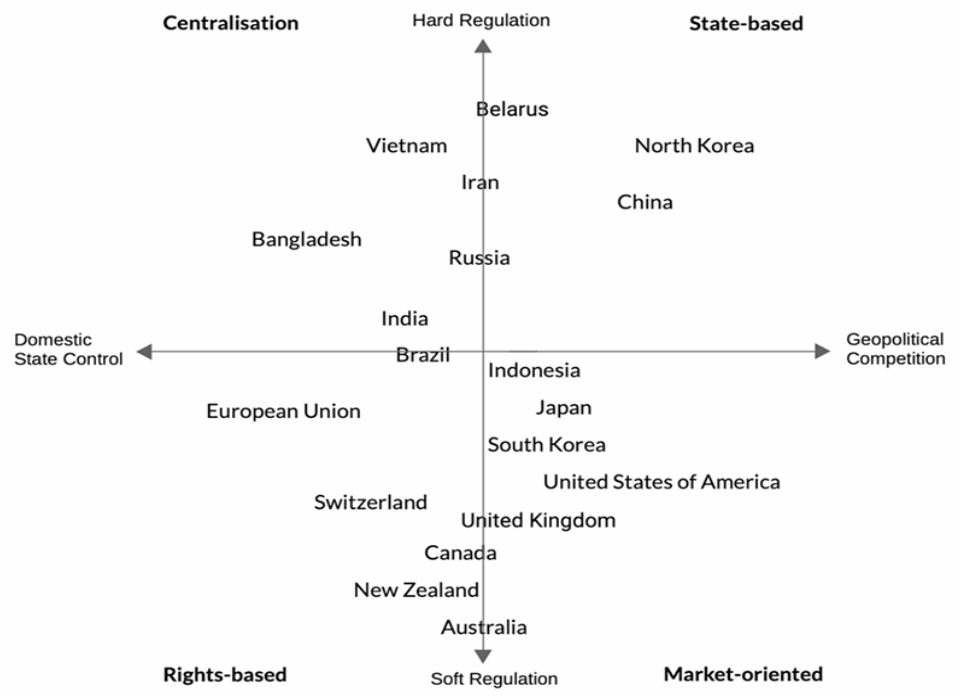
Value codes	**Right-based**	**State-based**	**Centralisation**	**Market-oriented**
Digital self-sufficiency		**X**	**X**	
State sovereignty over corporations	**X**		**X**	
Territorialization of cyberspace		**X**	**X**	
Nationalised governance		**X**		
Descriptive codes	**Right-based**	**State-based**	**Centralisation**	**Market-oriented**
Constraining corporate power	**X**		**X**	
Regulating digital innovation	**X**	**X**	**X**	
Reinforcing and securing infrastructures	**X**	**X**	**X**	**X**
Enforcing individual rights	**X**			
Engancing defense against cybercrime	**X**	**X**	**X**	**X**

Descriptive Analysis and a Critical Evaluation of Existing Models," *Digital Society* 3 (2024): 59,10,16.

Source : Adapted from Samuele Fratini, Emmie Hine, Claudio Novelli, Huw Roberts, and Luciano Floridi, "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models," Digital Society 3 (2024): 59,table 1.

The table below demonstrates that digital sovereignty models can be differentiated according to political logics and policy behaviours, expressed through value codes and descriptive codes respectively. The right-based model seeks to preserve sovereignty through the protection of individual freedoms and the limitation of corporate power, reflecting a liberal conception of governance in which legitimacy derives from rights and regulatory accountability,by contrast, the state-based and centralized models associate sovereignty with territorial control, nationalized governance and digital self-sufficiency, and treating cyberspace as an extension of state security and geopolitical competition. The market-oriented model links sovereignty to technological innovation, infrastructural competitiveness and private sector, yet despite the ideological differences, the convergence of all four models around cyber-security and infrastructure protection, which reflects that sovereignty in the AI era depends less on territorial authority and more on the capacity to secure and govern digital infrastructures, data flows, and computational systems.

Figure 6 : *Countries by model membership.*



Source : Samuele Fratini, Emmie Hine, Claudio Novelli, Huw Roberts, and Luciano Floridi, "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models," *Digital Society* 3 (2024): 59 ,fig.1.

The vertical axis captures the degree of assertiveness of state regulation, the horizontal axis distinguishes states whose objective is to design and enforce internal regulation from those that regulate digital intending to advance their geopolitical interests.

The figure illustrates a comparative mapping of national approaches to digital governance and sovereignty, structured along two main axes, first the degree of regulation from soft to hard, and the orientation of governance from right based to state based, as well as contrasting domestic state control with geopolitical competition. At the upper end of spectrum, countries such as China, North Korea and Belarus are positioned with the state-based model, characterized by strong centralization and hard regulation, which reflects a state-centric approach to digital sovereignty, where control over data, infrastructure and information flows is linked to political authority, digital sovereignty here is reinforced through restriction and centralized governance.

In contrast, countries like the United States, United Kingdom and Australia are located in the lower right side, representing a market oriented model, with softer regulatory frameworks. Digital sovereignty here is about enabling innovation, private sector leadership, and global competitiveness.

The European Union is located on the right based model and regulatory side, emphasizing data protection, ethical standards, and normative governance, which reveals that digital sovereignty is asserted through regulatory power.

Moreover, countries like India, Brazil and Indonesia are positioning in intermediate locations, reflecting hybrid approaches; these states combine elements of state control, market participation, and strategic adaptation.

Building on this analysis, digital sovereignty is a spectrum of governance models, shaped by political systems, economic priorities, and strategic objectives, also competing models coexist and interact, which shows that digital sovereignty is contested and reconfigured.

- **National AI Strategies :**
- **The United states National Strategy as a Market-oriented Model**

The United States pursues AI sovereignty through a market-oriented model that relies on private sector, American technological dominance was not produced by government planning but by private investment while the state’s role has been primarly protecting, extending and securing dominance rather than directing it. **The December 11, 2025 Executive Order Ensuring National policy Framework for Artificial Intelligence** reveals how the United States situates AI governance within a market-oriented digital sovereignty model. By implementing state-level regulations and establishing a federal framework, the order frames AI as a domain of national economic and geopolitical competition, emphasizing innovation and global dominance over fragmented regulatory oversight. The creation of an "AI Litigation Task force" shows a strategy

of consolidating authority at the federal level while minimizing regulatory burdens on private actors[1]. In addition to this, **the National AI Initiative Act 2020,** which marked a turning point in how the United States approached AI, rather than leaving progress to the private sector alone, Congress created a coordinated federal program to sustain long-term leadership in AI research, set standards for trustworthy and responsible use, and prepare the American workers for the changes that this technology would bring. The Act established the National AI initiative Office to align efforts across civilian agencies, defense, and intelligence, while also encouraging collaboration with international partners, which lead to a national strategy that combines innovation with democratic values.

In fact, the United States does not need to control AI in the way China does because American corporations: Google, Microsoft, Open AI, Amazon, Meta, already set global standards, with their dominant infrastructures, that's why market oriented model works for the U.S precisely.

China state-led strategy : the New Generation Artificial Intelligence Development Plan 2017 :

China's national approach to artificial intelligence reflects a state centric sovereignty model, in which technical development is linked to political authority, the new Generation Artificial Intelligence Development Plan(2017) set the ambition for China to become the global leader in AI by 2030, by leveraging the technology for economic growth and social governance. This strategy relies on central government but its execution is delegated to local government and national champion firms such as Baidu, Alibaba and Tencent. Creating a hybrid model of state guidance and corporate implementation.

Ethical frameworks emphasize collective stability and national priorities rather than individual rights. Digital sovereignty in this case is exercised through centralization, industrial mobilization and normative control[2].

This strategy has been complemented by regulatory instruments, for instance the **Algorithm Recommendation Regulations 2022** that targets recommendation systems,[3] and **the Generative AI Regulations 2023**, that addresses large language models and generative systems, with introducing obligations aroud AI generated content[4]. Digital sovereignty in this context is achieved through state control, however this strategy costs openness, which is essential in this interconnected international system.

---

[1] Donald J. Trump, *Ensuring a National Policy Framework for Artificial Intelligence,* Executive Order, December 11, 2025, The White House, https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy.

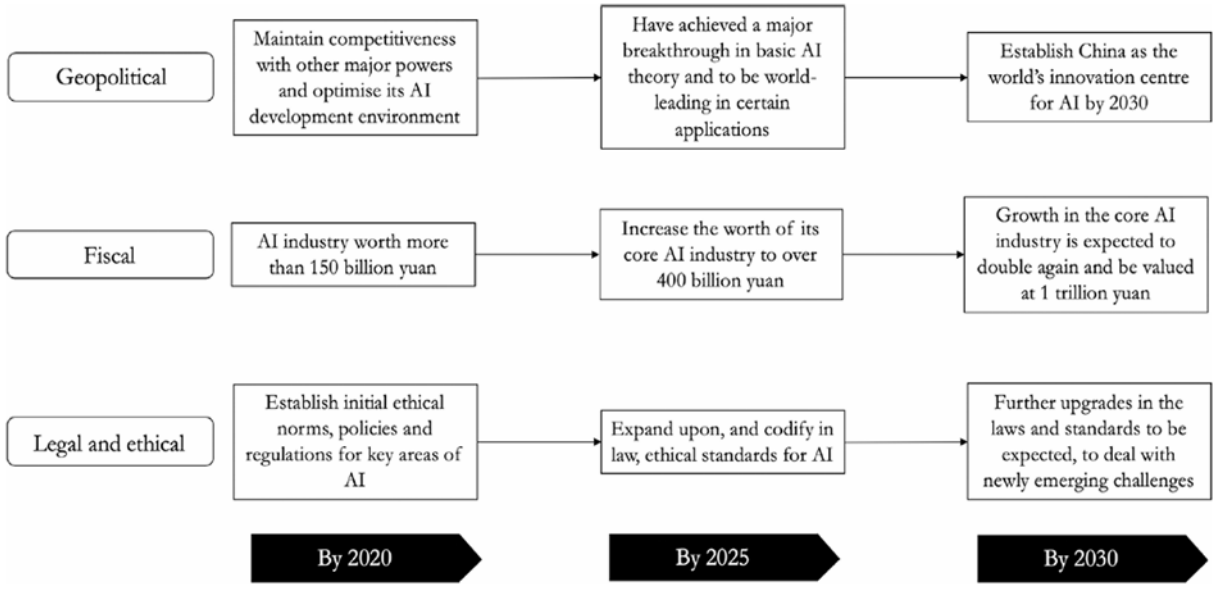
[2] Huw Roberts et al., "The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation," *AI & Society*, 2021, 72.

[3] Jian Xu, "Opening the 'Black Box' of Algorithms: Regulation of Algorithms in China," *Communication Research and Practice* 10, no. 3 (2024): 288–296,

[4] Mimi Zou and Lu Zhang, "Navigating China's Regulatory Approach to Generative Artificial Intelligence and Large Language Models," *Cambridge Forum on AI: Law and Governance* 1, no. 1 (2024): 1–20,2.

[1]. Digital sovereignty in this context is achieved through state control, however this strategy costs openness, which is essential in this interconnected international system.

Figure 7. Visualising China's AIDP



Source : ***Yi Zeng et al., "The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation," AI & Society, 2021,fig.1.***

The figure presents an overview of China's Artificial Intelligence Development plan AIDP, the strategy relies on three pillars : geopolitical positioning, economic expansion, and legal-ethical governance, between 2020, 2025 and 2030, from a geopolitical perspective, the plan emphasizes competitiveness with major powers and the ambition to achieve global leadership in AI innovation by 2030, which situates AI within a strategic rivalries. Economically, AI is used to increase economic development, and at the legal and ethical level, the strategy begins with establishing initial norms and policies and evolves toward upgrading laws and standards.

Beyond these dominant models, several countries launched their national AI strategies:

Russia's National AI Strategy

"Whichever country becomes the leader in artificial intelligence (AI) will become the ruler of the world" Russian Federation President Vladimir Putin-2017

Russian strategy relies on leveraging AI in defense, science, medicine and industry, this strategy reflects a distinctive model in which the Kremlin refrains from direct leadership, instead

[1] Mimi Zou and Lu Zhang, "Navigating China's Regulatory Approach to Generative Artificial Intelligence and Large Language Models," *Cambridge Forum on AI: Law and Governance* 1, no. 1 (2024): 1–20,2.

delegating responsibility to state owned firms. Unlike the United States and China, where private technology giants collaborate with government [1].

India's AI Development Strategy of 2018 prioritized five sectors: healthcare, education, agriculture, infrastructure, and transportation, which reflects India's objectives to use AI for social development and economic modernization**.**

Germany's national strategy of 2018 focuses on boosting national competitiveness while ensuring AI alignment with ethical standards and cultural values. The roadmap identifies 116 standardization needs and five regulatory priorities, including harmonization with EU law and AI security requirements. Which reflects Germany's approach of maintaining technological innovation with a strong legal and ethical framework.

Canada's Pan Canadian AI Strategy of 2017 established a national framework for AI development, later reinforced by the creation of an AI Advisory Board 2019 that included representatives from high-tech businesses and application developers[2].

The UAE strategy presents a clear vision, to establish the country as a global leader in AI by 2031, it emphasizes building a developed AI ecosystem, attracting and training talent and empowering economy. This strategy targets key sectors; administration, government, manufacturing, construction, healthcare, education, ICT and financial services. This NAS is part of UAE's strategy to become the "best country in the world" by 2071 [3].

3.1.2. Regional and Global AI Strategies

- **The European Union's Right-Based AI strategies :**

The European Union pursues a different strategy that rests on shaping global AI development by setting the standards that Bradford calls « **the Brussels Effect** », which means the capacity oft he EU to export ist regulatory standards globally through market access conditions. Beginning in **2018, the European Commision AI strategy** was the EU's first major step, setting out a vision that AI should serve people, not just markets. It emphasized ethics, trust, and investment in research. **The 2018 coordinated plan on AI [4]** focused on aligning national

[1] Petrella, Robert, Miller, Chris, and Cooper, Samuel. "Russia's Artificial Intelligence Strategy: The Role of State-Owned Firms." *Orbis* 65, no. 1 (Winter 2021): 77–95 , 75,76.
[2]Buriaga, V. O., V. V. Djuzhoma, and E. A. Artemenko. "Shaping an Artificial Intelligence Regulatory Model: International and Domestic Expe
rience." *Legal Issues in the Digital Age* 6, no. 2 (2025): 50–68. , 52,53.
[3] Arab Reform Initiative, "AI in the National: AI Strategies of the Arab Region," *Arab Reform Initiative*, April 2025, https://www.arab-reform.net/publication/ai-in-the-national-ai-strategies-of-the-arab-region/?tztc=1.
[4]eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52018DC0795 .

strategies, later **updated in 2021**[1], it focused on data availability, skills and sector specific applications.

The AI Act 2024[2] was the world's first comprehensive AI law, instead of vague principles, the EU now had binding rules, banning manipulative practices, regulating high-risk systems and requiring transparency for general purpose AI, its implementation between 2025 and 2027 focuses on advancing innovation while ensuring citizens are protected from AI risks.

The European Union's strategy is based on ethical responsibility, democratic reassurance, and a normative approach. However, this strategy risks being performative.

ASEAN's AI Strategy

The Association of the Southeast Asian Nations has adopted a pragmatic governance approach toward AI through its **ASEAN Guide on AI Governance and Ethics**, rather than focusing exclusively on technological competition the guide focuses on the responsible and trustworthy development of AI systems across the region. The strategy is based on key principles: **transparency**, **explainability** which refers to explaining how AI systems work in desicion- making process outside the black box[3] , **fairness**, **accountability and integrity**, **privacy**, **security**, and **human centric governance**, reflecting an effort to balance ethics with innovation. ASEAN also points out that AI governance should remain adaptive to AI constant development, particularly generative AI, whose risks the spread of misinformation, bias, privacy violations, and algorithmic opacity. Moreover, the Guide suggests the creation of **ASEAN Working Group on AI governance** to facilitate cooperation between member states, the strategy also encourages investment in AI research, digital infrastructure, cyber- security, invest in AI talents and start-ups, in addition to raising public awareness to reduce social vulnerability to AI risks [4].

However, this model is based on soft law frameworks which establish shared norms but cannot enforce them.

- **The African Union's Strategy :**

The African Union adopted its Continental Artificial Intelligence Strategy in 2024, which focuses on AI governance, ethics, human rights and digital sovereignty. It also stresses the

[1] European Commission. *Coordinated Plan on Artificial Intelligence 2021 Review*. Brussels, 15 December 2021 .

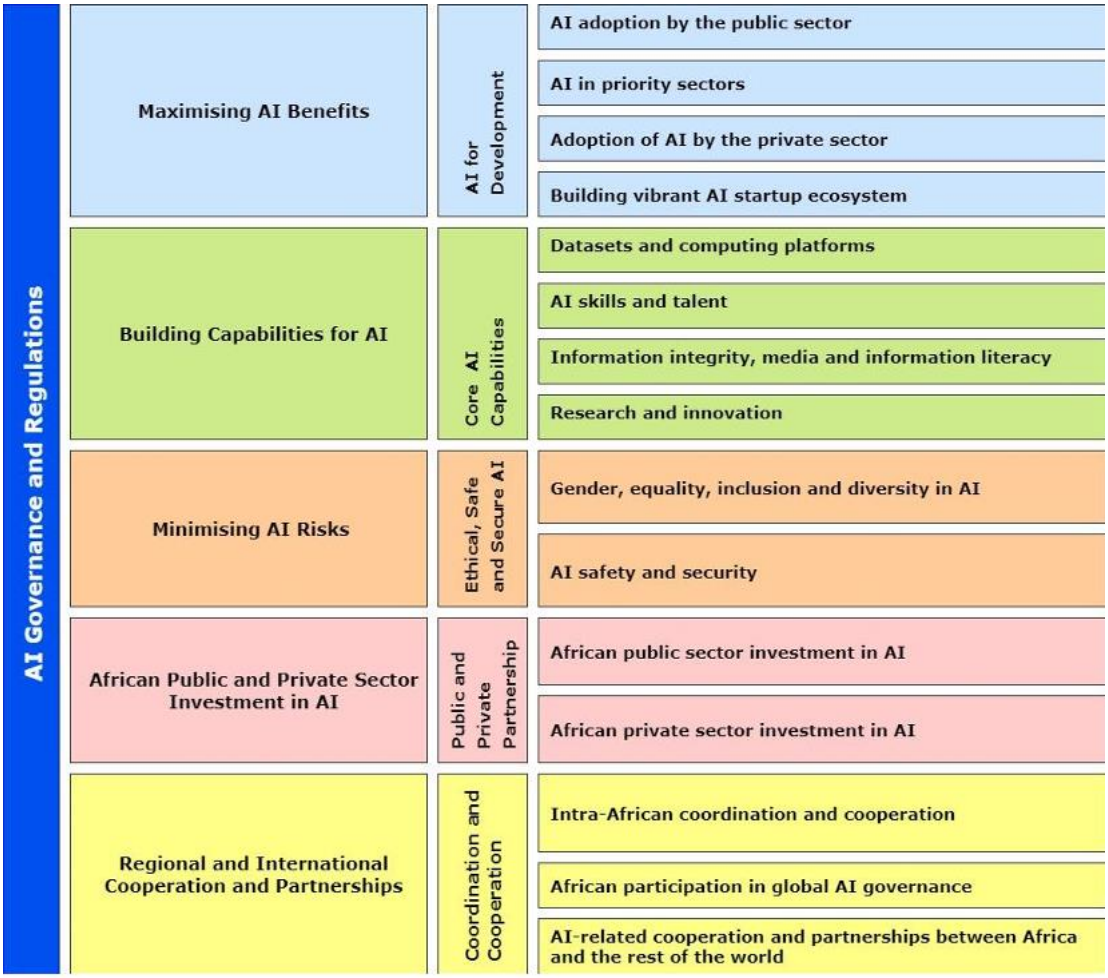
[2] « AI Act | Shaping Europe's Digital Future ».

[3] Association of Southeast Asian Nations, ASEAN Guide on AI Governance and Ethics(Jakarta: ASEAN Secretariat,2024), 35.

[4] Association of Southeast Asian Nations, ASEAN Guide on AI Governance and Ethics(Jakarta: ASEAN Secretariat,2024) ,3,8.

importance of developing local AI ecosystems and strengthening African control over data and digital infrastructures[1].

Figure 8 . Focus areas and action areas for the AI Strategy:



Source : African Union, Continental Artificial Intelligence Strategy for Africa(Addis Ababa: African Union, 2024)

The figure above represents the main pillars of the African Union ‘s continental AI strategy, reflecting a multi-dimensions approach that combines technological development, governance, capacity-building and international cooperation. Notably, the strategy insists on leveraging AI through public sector adoption, private-sector participation, startup ecosystems and AI application in priority sectors.

Moreover, the strategy points out the importance of building domestic capabilities, particularly through investments in datasets, computing infrastructure, AI skills, research and innovation, which reflects the awareness that digital sovereignty cannot be achieved only through regulation, but also requires technological capacity and local expertise. Another dimension on minimizing AI risks focuses on ethical and secure AI governance, by focusing on norms such

[1] African Union, Continental Artificial Intelligence Strategy for Africa(Addis Ababa: African Union, 2024), 3,5.

us integrity, safety, equality and gender. This rights oriented approach is an attempt to avoid reproducing old colonial patterns through technological domination.

Another dimension accentuates the regional and international cooperation, by emphasizing intra-African coordination and participation in global AI governance.

3.1.3.Global AI Strategies

- **United Nations Report : Governing AI for Humanity :**

The United Nations report governing AI for Humanity focuses on inequality, accountability, development, and geopolitical power. It points out how AI can accelerate progress on the sustainable development goals by improving health systems, agriculture and energy use but also warns that these benefits risk being captured by a small number of states and corporations, leaving many communities excluded. The report points out dangers such as bias, surveillance, disinformation, and autonomous weapons. Accordingly, AI's borderless nature demands a truly global response, by calling for a new social contract around AI, to ensures innovation, serve humanity equitably, protects right, and strengthen trust rather than eroding it[1].

The Global Digital Compact (Annex I, Pact for the Future) sets out a vision for an inclusive and sustainable digital future, through international cooperation and human rights. It emphasizes that digital technologies should serve as enablers of the Sustainable Development Goals by closing connectivity gaps, fostering digital literacy and ensuring that vulnerable communities are not left behind. The compact outlines commitments to universal and affordable internet access by 2030, investment in resilient infrastructure, and the promotion of digital public goods such as open-source software[2].

The UNESCO Recommendation on the Ethics of Artificial Intelligence is the first global standard-setting instrument on AI ethics, adopted by all member states in 2021. It approaches AI as a powerful technology with high potential but also profound risks, and sets out a roadmap for responsible governance. It focuses on core aspects: human dignity, environmental sustainability, fairness and inclussiveness.[3]

The OECD AI principles, adopted in 2019 and updated in 2024The OECD AI principles, adopted in 2019 and updated in 2024, were the first intergovernmental standard on AI, it focuses on five key aspects :

Inclusive growth, sustainable development and well being, human rights and democratic values including fairness and privacy, transparency and explainability, Robustness, security and safety and last Accountability.

[1] Vereinte Nationen, *Govering AI for Humanity*, 7,10.
[2]United Nations. *Annex I: Global Digital Compact, Pact for the Future*. New York: United Nations, 2024. .
[3]UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO,2021 . Ethics of Artificial Intelligence - AI | UNESCO

Practically it sets recommendations for policy makers that includes: investing in AI research and development, fostering an inclusive AI enabling ecosystem, shaping an enabling interoperable governance and policy environment for AI, Building human capacity and preparing for labour market transformation and international cooperation for trustworthy AI[1].

3.2.Sovereign AI, Data Localization and Cybersecurity

The governance frameworks examined previously represent the institutional framework through which states attempt to assert digital sovereignty, however regulations without instruments are not really effective, this section examines three practical digital sovereignty instruments : sovereign AI, data localization and cyber- security sovereignty

3.2.1. Sovereign AI

The notion of sovereign AI, refers to the idea that countries should build and sustain independent AI capabilities rather than depend on systems owned by foreign powers or multinational corporations, emerged around 2020, particularly in European debates on digital sovereignty and data protection. The concept gained more visibility when Nvidia's CEO Jensen Huang emphasized it during an earnings call in late 2023, consequently, a wave of global initiatives emerged under the banner of AI sovereignty. In essence, sovereignty in this context means a state's ability to develop and operate AI technologies on domestic infrastructure, using local data and expertise, without reliance on external platforms. Genuine sovereignty requires control over the entire AI lifecycle, from data collection and model training to deployment and governance, ensuring independence from foreign influence[2].

Sovereign AI can be defined across four pillars:

- **Data (D):** control over datasets, including ownership, governance and localization
- **Compute infrastructure (C):** chips, servers and sovereign cloud infrastructure
- **Model autonomy (M):** autonomy in developing and maintaining large language models and foundation models
- **Norms (N):** embedding local languages, values and cultural priorities into AI systems.

Building on that, AI sovereignty is expressed as a function:

$$S=f(D,C,M,N)^{3}$$

Which means that AI sovereignty (S) depends on how a country develops and balances these four pillars. For example, Indonesia may have strong talent but limited compute infrastructure,

[1] AI principles | OECD .
[2] Robert Dale, "Sovereign AI in 2025," *Natural Language Processing* 31 (2025): 1312–1321, Cambridge University Press, 1312.
[3] Singh et Sengupta, « Sovereign AI », 5.

so their sovereignty depends on managing these interdependencies strategically. Therefore, sovereign AI isn't just about having one resource like data or chips, it's about maintaining all four pillars together: data, compute, models and norms, and without investment and coordination sovereignty can't be sustained.

- **Why do states seek AI sovereignty?**

Nations seek sovereign AI for several reason, from a **national security** perspective, reliance on foreign built systems can expose critical infrastructures to vulnerabilities. Moreover, keeping **data within domestic borders** strengthens privacy protections against external legal frameworks. In addition, building local capabilities enhances economic competitiveness. **Regulatory autonomy** is another motivation, since global standards shaped by powerful foreign actors may overlook local priorities such as transparency, accountability and fairness. Equally important is **cultural and linguistic representation**, as models trained on local data are more convenient to education, services and knowledge specific to the population. **Strategic autonomy** equally, becomes essential in times of geopolitical tensions or trade wars, when dependence on external providers for essential functions could be dangerous[1].

- Can states achieve AI sovereignty?

Achieving the so-called **"full stack sovereignty"** in AI implies complete technological self-sufficiency across the entire ecosystem. Which encompasses several critical layers: the data used to train models, the models themselves, the GPU clusters that enable training and inference, and the cloud data centers that host this infrastructure. Each of these components is embedded in complex supply chains with their own dependencies; data centers require land and energy, chips depend on advanced design and photolithography equipment, and model development relies on research capacity and skilled talent.

Even in the leading AI powers, the United States and China, face challenges in securing autonomy at every level. While Nvidia and Huawei dominate chip design, both rely on external foundries such as TSMC and SMICA, which in turn depend on lithography machines produced by ASML in the Netherlands or SMEE in China. China maintains dominance across all layers of the stack, whereas the U.S lacks domestic lithography system manufacturers but retains influence through its control of key subsystems and its leverage over ASML[2].

Currently, ASML's monopoly on extreme ultraviolet lithography gives the U.S. the leverage because these machines are the only ones capable of producing the most advanced chips at 7 nanometers and below. Without EUV, China cannot fabricate cutting edge semiconductors, even in the Netherlands but relies heavily on U.S. components and subsystems, Washington can pressure ASML to block sales to China. Which creates a specific chokepoint advantage:

[1] Dale, « Sovereign AI in 2025 », 1312,1313.
[2] Dale, « Sovereign AI in 2025 », 13131,1314.

The U.S. indirectly controls access to EUV machines, while Taiwan's TSMC, which uses ASML's EUV systems can continue producing advanced chips for Nvidia and other U.S. firms.

China, by contrast is stuck with older deep ultraviolet (DUV) technology limiting its ability in chips production[1].

Within the European Union, sovereign AI has become tied to concerns over technological autonomy and strategic dependence on American corporations. The EU launched large scale initiatives such as the "AI factories" and "InvestAI" programs, simultaneously, the European Union attempted to promote locally developed AI models that reflect European languages and regulations, notably the French company Mistral AI and the OpenEuro LLM initiative.

At the semiconductor level, European governments have attempted to strengthen domestic chip production through projects like Openchip in Spain and SiPearl in France, while also attracting external investment from companies like Intel and TSMC. Yet, despite these efforts, European AI infrastructures continue to rely on external funding, foreign semiconductor supply chains, and American cloud providers which reflects the difficulty of achieving full technological autonomy[2].

The Middle East has adopted a more investment driven strategy that seeks to strengthen infrastructure. In terms of data centers, countries such as the United Arab Emirates and Saudi Arabia have partnered with firms including Amazon Web Services, Microsoft, and Open AI to establish large scale AI infrastructure projects. At the chip level, both states have invested in acquiring advanced AI processors from Nvidia and have explored semiconductor manufacturing partnership with TSMC and Samsung Electronics. While in AI models, the UAE's Flacon models and G42's Arabic language systems, which reflect the efforts to develop regionally adapted AI technologies. However, sovereign AI projects here remain integrated into American technological ecosystems and global semiconductor supply chains[3].

In Southeast Asia and India, sovereign AI strategies rely on state investments and partnerships with foreign technology firms. Many states have targeted the construction of national or regional AI infrastructure through investments by Google, Microsoft, and Nvidia.

South Korea and Japan have also expanded investment in semiconductor industries in attempt to preserve strategic technological autonomy.

Concerning AI models, countries across the region emphasize linguistic localization, for instance Indonesia's Sahabat-AI, Singapore's SEALION initiative, and India BharatGen and project Indus[4].

Africa's efforts to build a sovereign AI ecosystem remain constrained by limited financial resources, weak infrastructure and conflicting regulatory frameworks. Both the United States

[1] Dale, « Sovereign AI in 2025 », 1314.
[2] Dale, « Sovereign AI in 2025 », 1314,1316.
[3] Dale, « Sovereign AI in 2025 »,1317,1318.
[4] Dale, « Sovereign AI in 2025 »,1318,1319.

and China are competing to dominate in this area, with Beijing's 2025-27 action plan, that paved the way to Sino-African cooperation in technology, including digital infrastructure. Major investments such as Microsoft, in partnership with UAE-based G42 pledged 1 billion dollars for a Kenyan data center in 2024, and an additional 300 million dollars for facilities in South Africa. AWS and Google have also established data centers in South Africa, while AWS has announced plans to expand cloud services to Morocco and Senegal, though these are not yet AI specific. Local initiatives exist but remain dependent on Western technology. Cassava technologies for instance, plans to build Africa's first AI factory using Nvidia Chips, beginning in South Africa and later extending to Egypt, Kenya, Morocco and Nigeria. Africa Data Centers previously announced a 500 million dollars program to construct ten interconnected hyper-scale data centers, though progress has been slow. On the model side, homegrown startups are emerging, such as South Africa's Lelapa AI has released InkubaLM, a multilingual LLM covering Swahili, Yoruba, isiXhosa, Hausa and isiZulu: Kenya's Jacaranda Health has introduced UlizaLlama for Swahili; and Nigeria's EqualyzAI is developing culturally attuned models that reflect African languages and context[1].

The critical assessment of sovereign AI as a sovereignty instrument reveals that states face serious challenges, the cost barrier for instance, makes sovereign AI practically unachievable for most states, because training AI models requires billions of dollars in compute investment, vast quantities of high quality training data, however for states that already occupy the dominant positions in global AI sovereign AI is achievable, which reproduces rather than resolve dependency gaps.

3.2.2.Data Localization

Data localization refers to the state’s efforts to keep data within their territorial boundaries. At its core, it is about asserting jurisdictional control over where information can be stored, processed or transferred[2].It can be defined also as the « forced local data-residency requirements that confine data within a country’s border »[3] .

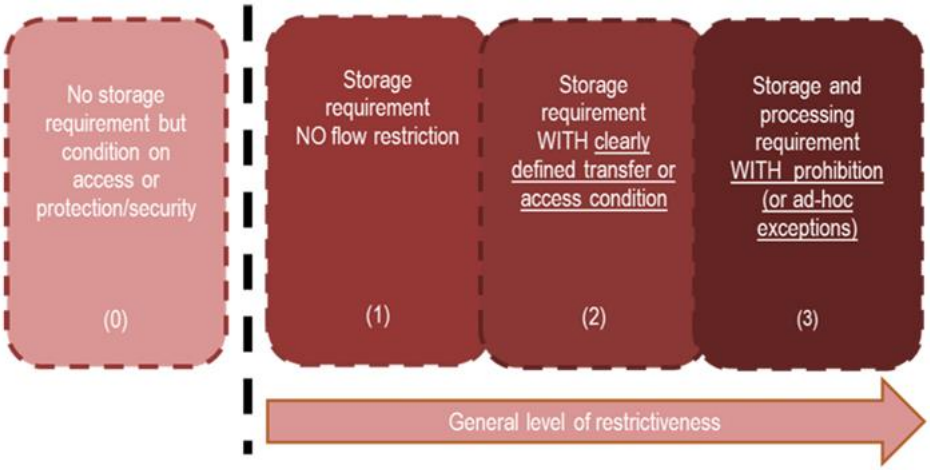
Data localization may take three forms: certain frameworks require that data be stored domestically but still permit duplication and processing abroad, thereby ensuring national access without fully restricting international flows. Sweden's Accounting Act represents the minimalist version, where regulators want jurisdictional reach, but they allow the global circulation of data.

A more restrictive model obliges local storage while allowing cross-border transfer or processing under clearly defined legal or contractual safeguards. Australia represents this model, by insisting on domestic storage but allowing transfers under strict safeguards. At the

[1] Dale, « Sovereign AI in 2025 »,1320.
[2] Jyoti Panday and Jeremy Malcolm, *The Political Economy of Data Localization* (ResearchGate, 2018):513.
[3] *A Preliminary Mapping of Data Localisation Measures*, 262,5.

most rigid level, some regimes mandate they both storage and processing occur fully within national borders, prohibiting transfers abroad except in narrow circumstances[1]. In this context, China and Indonesia turn data localisation into a sovereignty matter, data in this models must be managed, processed and stored locally.

Figure 9 . A typology of data localization measures and requirements for data flow



Source : OECD, A Preliminary Mapping of Data Localisation Measures, OECD Policy Paper No.262,2022.

The figure presents a typology of data localization measures and illustrates the different degrees of state restriction imposed on cross-border data flows .It demonstrates that data localization is not a uniform policy, but rather a spectrum of regulatory approaches, from limited oversight to strict territorial control over data storage and processing.

In addition to the previously mentioned categories, a new model of localization is emerging (the category 0), one that does not demand domestic storage but insists on guaranteed access. Mexico's telecommunications law, and the EU's regulation on non personal data embody this logic, where firms may store data wherever they wish, but they must ensure that regulators can reach it[2].

Data localization requirements are often justified as a means of safeguarding domestic privacy regimes and ensuring that the right of individuals is respected within national jurisdictions. In addition, states also view local storage as a way to guarantee regulatory access to information, whether for tax authorities seeking records or for sectorial regulators in telecommunications, banking, and insurance, who require current data to ensure operational compliance. Moreover, in the context of national security, localisation can facilitate domestic intelligence services access to sensitive information while simultaneously protecting it from foreign actors, also

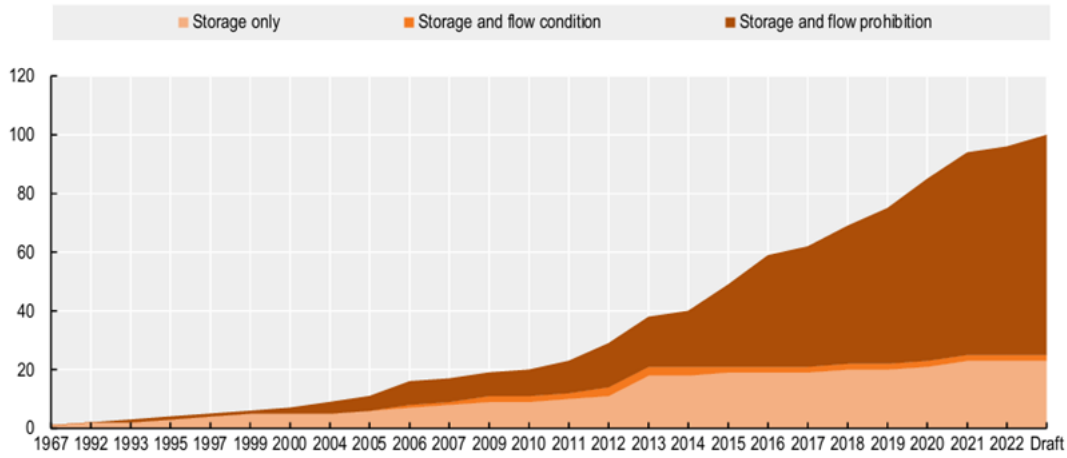
[1] *A Preliminary Mapping of Data Localisation Measures*, 262:6,7.
[2] *A Preliminary Mapping of Data Localisation Measures*, 262,8.

governments argue that data security is best assured when storage and processing remain within national borders, to reduce exposure to external vulnerabilities.

Furthermore, localization is increasingly deployed as an instrument of industrial policy or digital protectionism, with the expectation that mandating domestic storage and processing will strengthen local capacity[1].

In the AI era, data localization is not just about privacy or regulatory access, it is about power. Whoever controls the data controls the capacity to train, refine and deploy advanced AI models. Governments see data localization as a way to prevent foreign platforms from monopolizing domestic datasets, thereby seeking to assert sovereign over algorithms and reducing digital dependency. Yet this strategy is double edged, between openness and isolation, it can secure national security but isolate states from the global data flows that drive innovation.

Figure 10 . Data localization is growing and becoming more restrictive



Note: Data localisation measures are defined as explicit requirements that data be stored or processed domestically.
Source: Author's compilation based on own compilation including through the Digital Trade Alert, the OECD Digital STRI and Cory and Dascoli (2021[2]).

Source : OECD, The Nature,Evolution and Potential Implications of Data Localisation , OECD Trade Policy Paper No 262,2023.

By the early 2023, 96 measures were in force across 40 countries, with 4 more in draft form, and nearly half of them had been introduced only since 2015. What matters most is not just the growth in number, but the fact that more than two thirds of these rules fell into the most severe category, requiring domestic storage and prohibiting cross-border transfers. In other words, governments are treating data as strategic asset that must remain within national borders, which signals a move toward digital protectionism and sovereignty.

The figure above shows the expansion of data localization measures over time, while also demonstrating a trend toward restricitve forms of digital regulation, beginning in the late 1990's

[1] *A Preliminary Mapping of Data Localisation Measures*, 262,6.

and accelerating significantly after 2010, states have progressively adopted policies requiring data to be stored, processed or controlled within national territories. The most notable trend is the sharp growth after 2014, reflecting the politicization of data governance in the digital era, equally important, this trend reflects the shift in sovereignty as well, traditionally, it was exercised primarily through territorial control over physical space.However, in the digital age, states seek to extend sovereign authority into cyberspace through regulatory control over data circulation, in this context, data localization is a mechanism for adapting to the AI and digital era.

Data localization as a sovereignty instrument faces challenges that limit its effectiveness, for instance localization without local capacity is symbolic sovereignty, requiring data to be stored domestically does not create the AI development ecosystem necessary to exploit that data sovereignty.

Moreover, data stored domestically on servers owned by foreign corporations remains subject to the legal reach of those corporations home jurisdictions through instruments like the US CLOUD Act. Overall, true data sovereignty requires not only domestic storage but domestic ownership, a condition that most states are far from achieving.

3.2.3. Cybersecurity

As states become dependent on digital infrastructure, cybersecurity is no longer understood as a technical issue of network protection, but as a central dimension of sovereignty. The ability to secure national digital ecosystems, protect critical infrastructures, and control strategic data flows has become linked to the capacity of states to exercise authority in the digital age. In this context **cybersecurity sovereignty** refers to « the application of principles of state sovereignty to cyberspace »[1].

In the AI era, what distinguishes the contemporary cybersecurity from previous generations, is the fact that AI has fundamentally altered the offensive capabilities available to state and non state actors, creating a dual edged dynamic, the same AI capabilities that enhance defensive cybersecurity empower offensive operations in ways that traditional security mechanisms where not designed to counter. Scholars distinguish three specific transformations, first **AI-powered offensive capabilities,** whereby offensive AI systems autonomously scan attack surfaces, identify vulnerabilities, adapt to countermeasures in real time, and execute attacks without human intervention.

The second type is **defensive AI**, which operates as a shield, designed to anticipate and neutralize intrusions through systems like intrusion detection or automated malware analysis. In practice, this includes deep fake audio and video, misinformation bots.

Where offensive AI attacks external systems, **adversarial AI** attacks the AI systems states rely upon to govern, by poisoning training data, manipulating model outputs, inducing

[1] Marie Baezner et Patrice Robin, *Cyber Sovereignty and Data Sovereignty: Trend Analysis* (Zürich: Center for Security Studies (CSS), ETH Zürich, Risk and Resilience Team, novembre 2018) ,7.

misclassification in systems used for law enforcement, border control, healthcare and financial regulation. When a state deploys an AI system to make governance decisions an adversary can manipulate that system's output without detection, which makes the decisions made by compromised AI systems carry the formal authority of the state while serving interests of its adversaries[1].

In response to emerging cyber threats states implemented different cybersecurity sovereignty strategies, the United States for instance pursues offensive defensive integration, the doctrine that cybersecurity sovereignty requires active offensive capacity to disrupt adversaries before they can strike. **The 2023 U.S. National Cybersecurity Strategy** lays out five pillars that together form the backbone of America's approach to digital resilience. It begins with the protection of critical infrastructures, making sure that essential services like energy, healthcare and communications are not left vulnerable to disruption. It then turns to the active dismantling of malicious actors, signaling that the United States will not simply defend but will impose costs on those who threaten its networks. A third pillar focuses on shaping market forces to drive security and resilience, the fourth pillar focuses on investing in research and workforce development, the fifth pillar points out the importance of international partnerships[2].

The European Union pursues regulatory cybersecurity sovereignty through binding standards that the Brussels Effect can export globally.The Network and Information Security Directive **NIS2,2022** establishes mandatory cybersecurity requirements across member states and operators of critical infrastructure[3], while **the Cyber Solidarity Act 2024[4]** builds a collective European cybersecurity shield through AI-powered security operations centers.Yet, the EU regulates cybersecurity more comprehensively than any other actor in the international system while depending on American cybersecurity technology for its most critical defensive capabilities[5].

China has built a set of cybersecurity laws that are less about the technical details of networks and more about showing how the state claims authority over the digital world. **The Cybersecurity Law of 2016** was the first big step, it obliged companies to store data inside China, register users with real names, and allow the government to monitor online activity. Later**, the Data Security Law (2021)** added a system that ranks data by how sensitive it is, linking information management directly to national security. At the same time, **the Personal Information Protection Law (2021)** introduced rules for how companies handle personal data[6], similar to Europe's GDPR, but with wide exceptions that let government agencies collect and use data freely.

---

[1] Masike Malatji and Alaa Tolah,"Artificial Intelligence (AI) Cybersecurity dimensions: A Comprehensive Framework For Understanding Adversarial and Offensive AI" (2024) AI and Ethics 5 ,883.
[2] United States, National Cybersecurity Strategy (Washington, D.C.: The White House, March 2023), 4.
[3] Annegret Bendiek and Isabella Stuerzer, "The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate," European Political Science Review,January 23, 2023, 6.
[4] Council of the European Union, *Cyber Solidarity Act 2024: Strengthening EU Cybersecurity Capacities*, ST 08047 EN 24 (Brussels: Council of the European Union, 2024).
[5] Gineikyte-Kanclere et al., *European Software and Cyber Dependencies*, 16.
[6] Rogier Creemers, "Cybersecurity Law and Regulation in China: Securing the Smart State," China Law and

Equally important, what applies to sovereign AI and data localization applies to cybersecurity, these practical instruments are necessary but insufficient. They extend reach of existing power rather than redistributing it. They protect the sovereignty of states that already possess the capacity to defend themselves. And they leave the weaker states, structurally exposed in ways that no combination of current instruments can resolve.

This section mapped the responses to AI's challenge to digital sovereignty, national strategies are implemented but many remain limited in practice, regional frameworks have developed more comprehensive regulatory approaches, yet enforcement differs between states, for instance the EU regulatory framework is comprehensive but some states or companies comply more effectively than others. At the global level, international principles and ethical frameworks lack binding force and effective enforcement mechanisms.

Sovereign AI, remains a privilege of the dominant powers, data localization attempts to strengthen state control over data, but it also conflicts with the global and cross-border nature of the digital world .Moreover, cybersecurity sovereignty is structurally unachievable to the states that need it most.

This leads to a core question in this thesis, if current responses are inadequate to the depth of the challenge, what would an adequate response look like? and what practical transformations are genuinely necessary to achieve it?

3.3.Toward a New Model of Digital Sovereignty

Current responses to artificial intelligence reflect awareness of the strategic importance of digital sovereignty, states,regional and international organizations have developed regulatory frameworks, cybersecurity,AI and data strategies, however, structural limitations persist, notably for the global south.

3.3.1. The limits of Current Responses

Dismissing current efforts completely would be unfair, as there has been genuine progress in establishing norms. The fact that more than 90 nations have aligned on AI governance principles, even if they aren't legally binding, marks a real shift in how state sovereignty is defined in the digital era.Assessing current responses globally will be inadequate, it is more convenient to assess them through the four digital sovereignty models established in 3.1, because each model's limits are distinct :

Current responses to digital sovereignty illustrate the limits of existing governance models. The EU's **rights-based approach**, exemplified by the AI Act and GDPR, demonstrates adaptability through risk-based regulations but remains constrained by the slow pace of comprehensive law making, which risks stalling innovation.Also, the EU model cannot resolve through regulation alone, it governs technology produced mainly by the U.S and China, for instance, European

Society Review 6 (2021): 111–145. 121,123.

governments store sensitive data on American cloud infrastructure subject to the Cloud Act, also European AI applications depend on American or Chinese foundation models whose training data, design logic and update mechanisms outside European control, therefore the gap between regulatory ambition and sovereign reality is impossible to ignore, the European Union has built a solid regulatory framework but did not eliminate dependency fully[1].

The **market-oriented model**, often associated with the United States and its neoliberal legacy, holds deep contradictions between its rhetoric of laisez-faire innovation and the reality of persistent state intervention, while Silicon Valley firms's discourse is based on self-regulation and market freedom, their rise was enforced by state support.Moreover, the model reliance on self-regulation has historically weakened rights protection, leaving privacyand content moderation subordinated to free trade and market logic.In recent years, with bans on platforms like TikTok and restrictions on Huawei, national security concerns have eroded the laissez-faire ideology, also this model's expansionist dimension, illustrated in the U.S corporations and infrastructures export governance norms abroad, reinforces asymmetries in the global digital order, privileging American standards while constraining the autonomy of other states. Thus, the market oriented model's strength in innovation and global dominance is associated with weaknesses ; dependence on state intervention, vulnerability to geopolitical contestation, and reproduction of inequalities in cyberspace[2].

Centralisation, secures stability and national control but sacrifices inclusivity and adaptability, which undermines innovation and responsiveness to global trends, this model solves the political problem of external interference while creating the economic problem of technological stagnation. While effective in consolidating state authority, this model raises concerns regarding its broader implications for digital sovereignty, by excluding non-state actors and foreign platforms, governments risk fostering isolationist tendencies that undermine innovation and connectivity, Russia's bans on western platforms and the promotion of domestic alternatives such as VK and Yandex is a clear evidence in this regard,Iran and Bangladesh follow the same pattern, which secures non interference but supress and shape public opinion[3].

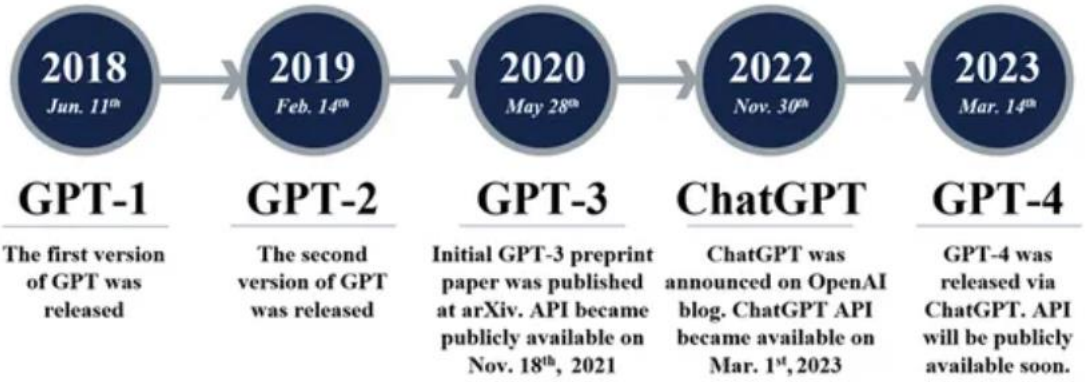
State-centric model, followed by Chinese strategies, mobilise vast resources and foster innovation, but blurs public-private boundaries, limiting participatory governance, and creates a system where corporations function as extensions of state power rather than independent actors, which increases dominance over cyberspace while leaving no marge for civil society or alternative governance voices, as a result it creates a closed state centric cyberspace that prioritises regime stability and geopolitical competition over openness, innovation and global interconnectivity[4].

The previously mentioned frameworks are not flexible, they were designed for a technological environement that no longer exists by the time it is implemented. **The EU AI Act** took four

[1] Samuele Fratini, Emmie Hine, Claudio Novelli, Huw Roberts, and Luciano Floridi, "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models," *Digital Society* 3, no. 59 (2024): 1–27, 12.
[2] Fratini et al., « Digital Sovereignty », 13.
[3] Fratini et al., « Digital Sovereignty », 14,15,16.
[4] Fratini et al., « Digital Sovereignty », 16.

years to negotiate implementation[1], in the same period, AI capabilities have advanced from GPT-3 to GPT4 systems whose reasoning capabilities exceed human performance on a growing range of tasks[2].The OECD AI principles were adopted in 2019, before large language models existed at commercial scale.

Figure 11. Generative AI's Shift



Source : Analytics Vidhya, Generative AI's Shift From GPT-3.5 to GPT-4 Journey

This shows **the gap between implementing policies and the speed of algorithmic development** and the speed of democratic governance, legislative processes require deliberation, consultation, negotiation, and implementation. All of which take time that AI development does not provide, consequently, governance frameworks are regulating old AI while new technologies are already being deployed, this speed asymmetry requires a different approach to governance that builds adaptability into the framework, rather than being outpaced by new AI models[3].

Another problem is that global AI governance has been built for the states that already dominate AI development, the United States, China and the European Union. Standards set by powerful states that developing states must adopt as a condition of digital participation, without input in their design or a capacity to enforce them domestically and without the technological infrastructure, are just a form of regulatory hegemony.

Reaching a global consensus on artificial intelligence guidlines is also a challenge to global digital order, the diversity of legal traditions, cultural values and ethical priorities across regions means that no single framework can easily accommodate all perspectives, the plurality of approaches analysed in the different responses requires not only negotiation but also a nuanced lens of these varied perspectives[4].

[1] Consilium, « Artificial Intelligence Act » Artificial intelligence act - Consilium.
[2] Dash, « Generative AI's Shift From GPT-3.5 to GPT-4 Journey ».
[3]Yoshija Walter, "Managing the Race to the Moon: Global Policy and Governance in Artificial Intelligence Regulation-A Contemporary Overview and an Analysis of Socioeconomic Consequences," Discover Artificial Intelligence, 2024. , 12.
[4] Walter, « Managing the Race to the Moon », 2.

The limitations across the four models: regulatory sovereignty without technological autonomy, market dominance without accountability, state control with isolation, in addition to speed gap, cultural challenges and structural inequality, come from a deeper issue, the way that sovereignty is conceptualized, in the AI era power is deterritorialized, trying to govern AI only with territorial state logic is incorrect, governance models should match the nature of AI.

Building on that, what does an adequate response look like ?

An adequate response to AI governance does not consist in replacing the state, but in redefining sovereignty in ways capable of integrating infrastructural dependency, transnational digital networks, and multi-level governance structures. Digital sovereignty in the AI era should no longer be understood as territorial authority exercised by states within fixed borders, instead it depends on the capacity to govern digital infrastructures, secure data ecosystems, regulate transnational technological actors and maintain strategic autonomy within the interconnected networks, therefore it becomes:

- **Functional and infrastructural**, not only measured by territorial control but by control over data, AI capabilities, infrastructures, cloud systems.
- **Networked**, AI governance must include international coordination and binding transnational accountability mechanisms
- **Hybrid,** distributed between states, corporations and international organizations.

3.3.2. Policy Recommendations for the Global South

Studying digital sovereignty in the Global South cannot be treated as a coherent or uniform category, as levels of technological capacity, infrastructural dependence, AI integration, and regulatory development differ significantly between states, the challenges faced by Brazil, Algeria or South Africa are not identical. Thus, policy responses to AI governance and digital sovereignty cannot rely on universal models. However, although many of these states remain exposed to similar challenges related to infrastructural dependence, limited AI resources, and unequal integration to the global digital economy. In this context, the following recommendations aim to strengthen digital sovereignty in the face of growing digital asymmetries :

First, developing countries must strengthen local digital infrastructures, including data centers, cloud storage systems, and computational processing capacities, because without domestic infrastructures capable of storing, processing, and governing data, claims of digital sovereignty remain largely symbolic. In practice, dependence on foreign technological infrastructures limit state's capacity to exercise control over strategic digital resource. In this context, the UNCTAD Digital Economy Report 2021 emphasizes that investment in data collection, storage, and

processing infrastructures constitute a pillar for domestic digital industrialization and long term technological development. Consequently, data localization policies alone are insufficient if they are not accompanied by investments in national technological capabilities and digital ecosystems.

Second, developing countries should push for a more inclusive global digital governance architecture capable of addressing existing structural inequalities within the international digital order, as current governance frameworks remain influenced by dominant powers and large digital corporations, which limits the capacity of global south countries to shape emerging AI norms and standards, enforcing the representation of developing countries within international digital governance institutions therefore becomes essential in order to avoid reproducing new forms of technological dependency and marginalization. In this context, South-South cooperation constitute an important mechanism for reducing asymmetrical dependency relations.

Third, as the Global South states are often marginalized in the production of core technologies, the establishment of dedicated « **tech-diplomacy**»[1]

mechanisms offers a pragmatic way to reclaim agency, appointing specialized ambassadors or envoys tasked with negotiating directly with major technology companies and host governments would ensure that these countries are not passive recipients of external standards but active participants in shaping them, such representatives could defend national and regional interests on issues of data governance, platform accountability and digital rights, while also pushing pushing back against exploitative practices linked to digital colonialism and extractive capitalism, in this way tech-diplomacy becomes a strategic instrument for sovereignty, even if the Global South cannot yet compete technologically, it can negotiate the terms of engagement, assert its normative priorities and secure a more equitable position within the digital order.

Finally, asserting digital sovereignty starts from investment in local research, education and AI start ups, because technological dependency is not only infrastructural but also epistemological, states that rely on foreign technologies risk remaining structurally dependent, therefore supporting domestic scholarship and research capacities becomes a strategic dimension of sovereignty, allowing developing countries not only to consume technological systems but also participate actively in shaping governance structures.

The structural conditions that produce digital dependency will not be altered by better national strategies alone, or by more inclusive multilateral principles alone, they require the combination of domestic investment, collective action, and self-determination that the three pillars proposed here represent.

[1] Andrew Mazen Dahdal and Adel Abdel Ghafar, "The Digital Silk Road: 'Tech-Diplomacy' as a Paradigm for Understanding Technological Adoption and Emerging Digital Regulations in MENA," *Asian Journal of Law and Society* 12 (2025): 163–188,167.

Findings of Part Three :

This chapter demonstrated that states seek to assert digital sovereignty through mechanisms such as national strategies, regional frameworks, international initiatives, sovereign AI, data localization and cybersecurity, however these responses remain shaped by significant asymmetries in technological capacity, economic power, and geopolitical influence. Moreover, current governance models face limitations, regulatory sovereignty without technological autonomy, market dominance without accountability and state control without global interconnectivity, in this context, effective digital sovereignty depends on the the capacity to secure infrastructures, govern data flows and strengthen cybersecurity resilience, and develop domestic technological capabilities, for developing countries, it is important to work on reducing structural dependency by investing in education, research, regional cooperation and South-South alliances**.**

Conclusion

Conclusion

This thesis has investigated the profound reconfiguration of state sovereignty in the contemporary international system, driven by the rapid expansion of artificial intelligence (AI) and global digital ecosystems. Historically defined by territorial boundaries, physical jurisdictions, and a state monopoly on legitimate authority, the concept of sovereignty is facing an unprecedented existential crisis. This study addressed a pivotal question: *How does artificial intelligence reconfigure the concept of sovereignty in the digital age, and what conceptual, theoretical, and practical changes are required to navigate this transition?* By examining the shift from traditional land-bound authority to the governance of transnational data flows, computational platforms, and technological infrastructures, this research sought to unpack how the intersection of AI and digital networks disrupts the classical Westphalian model of the state.

The empirical and conceptual analysis conducted across this study yielded several major insights regarding the contemporary global digital order:

The Rise of Computational Power Materiality: Far from existing in an immaterial cloud, digital power is deeply anchored in a physical and highly concentrated megastructure of hardware, including submarine fiber-optic cables, massive localized data centers, and advanced semiconductor manufacturing hubs.

The State-Corporation Power Redistribution: Multinational technology corporations have transcended the role of market actors to become sovereign-like entities. Through their exclusive control over algorithmic design, hyperscale cloud structures, and generative AI models, these firms now dictate the operational and security frameworks that states rely upon.

Geopolitical Asymmetry and the Tech Duopoly: The global distribution of AI capabilities has intensified a bipolar technological rivalry between the United States and China, consolidating a global digital hierarchy. This dynamic has deepened the structural dependence of peripheral nations, particularly across the Global South, who are increasingly forced into a state of digital subordination where they provide raw data while remaining reliant on foreign computational intelligence.

In answer to the central research question and in confirmation of the hypothesis ,this thesis concludes that **digital sovereignty in the era of artificial intelligence can no longer be understood as absolute, strictly territorial, or exclusively state-centric; instead, it has been transformed into a hybrid, multi-layered, and relational form of infrastructural authority.** The final position of this thesis asserts that true sovereign power in the 21st century is determined by an actor's capacity to control and direct different vertical layers of the global computational architecture. Consequently, rather than resulting in the total erasure of the state, the AI era is forcing a profound reconfiguration where states must project authority *through* technology, legal standards, and digital localization policies, operating alongside private corporations in a highly contested and interdependent matrix of power.

Theoretically, these findings challenge and extend existing International Relations paradigms, reinforcing the necessity of the hybrid analytical framework established in this study.

Realism & IPE: While Classical and Structural Realism successfully explain interstate competition and the "weaponized interdependence" seen in chip export controls, their state-centric ontology fails to account for the sovereign agency of Big Tech. By integrating Susan Strange's International Political Economy (IPE) perspective, this study extends theory by demonstrating how "knowledge structures" and control over AI systems have surpassed military power as primary determinants of global authority.

Constructivism & Dependency Theory: This research supports the Constructivist view that sovereignty is a socially constructed, evolving norm, as evidenced by how European, American, and Chinese identities produce divergent regulatory models. Furthermore, it validates and updates Dependency Theory by illustrating that classical colonial resource extraction has mutated into "data colonialism," where the Global South faces structural inequalities rooted in algorithmic and computational asymmetries.

The practical and policy relevance of this research directly addresses the strategic autonomy of modern institutions and governments:

For Policymakers in the Global South: The study demonstrates that passive tech adoption breeds permanent strategic vulnerability. Peripheral states must move away from total reliance on foreign hyperscalers and invest in targeted "Sovereign AI" initiatives, domestic data localization frameworks, and regional cybersecurity standards to prevent technical disruptions from being weaponized against national interests.

For International Institutions & Regional Blocs: Practitioners can look to the European Union’s regulatory acts (such as the GDPR and the AI Act) as blueprints for exercising normative power. However, policies must recognize that legal frameworks remain fragile unless backed by material infrastructural investments, such as independent cloud capacities and localized data storage facilities.

This thesis contributes original insights to the academic field of International Relations by bridging the gap between classical political philosophy and critical technological materialism. While existing literature frequently separates technological capability from sovereign legitimacy, this study unifies them by mapping political authority directly onto contemporary computational frameworks, such as Benjamin Bratton’s architectural "Stack" model. It provides a unique, system-level categorization of how algorithmic governance directly erodes Westphalian boundaries, offering a robust, updated hybrid framework that allows scholars to analyze sub-state, corporate, and interstate power dynamics simultaneously.

Despite its rigorous framework, this study acknowledges clear boundaries:

Methodological Limits: Given the rapid pace of technological innovation, capturing the full operational impact of real-time developments in generative AI and quantum computing remains methodologically challenging.

Data Limits: Much of the corporate data regarding proprietary algorithms, AI private investments, and state-sanctioned cyber-capabilities remains classified or hidden behind

corporate confidentiality, forcing reliance on open-source institutional reports and secondary indices.

Scope Limits: The study focused primarily on the macro-geopolitical triangle of the US, China, and the EU, which may limit the granular applicability of the findings to highly specific local governance contexts in smaller developing states.

To advance the broader academic conversation, future scholarship should explore several remaining gaps in the digital sovereignty discourse:

Empirical Testing of Sovereign AI: Future studies should empirically measure the socioeconomic viability and performance of localized "Sovereign AI" models developed outside the Western and Chinese ecosystems.

The Role of Non-State Governance Transnational Alliances: Further research is needed to examine how non-state standards bodies (such as ICANN or IEEE) and cross-border civil advocacy networks can be leveraged to democratize global algorithmic governance.

Micro-Level Structural Dependency: Investigators should look beyond state-level analyses to evaluate how corporate cloud monopolies impact the domestic judicial and administrative autonomy of critical public institutions within developing nations.

In conclusion, the intersection of artificial intelligence and digital infrastructure has fundamentally unmoored sovereignty from its classical Westphalian foundations. The political architecture of the world is no longer drawn solely on physical maps, but is continuously written into data centers, undersea fiber-optic lines, and machine learning algorithms. As the international system transitions into a multipolar digital order, the ultimate metric of state power will not be measured merely by physical borders or conventional military deployment, but by the structural capacity to command computational intelligence. For the modern state, adapting to this hybrid paradigm is no longer a matter of technological luxury, but a core prerequisite for political survival and independent governance in the digital age.

BIBLIOGRAPHY

BIBLIOGRAPHY

- **Books**

1. Bartelson, Jens. **A Genealogy of Sovereignty**. Cambridge: Cambridge University Press, 1995.
2. Bodin, Jean**. Les six livres de la République**. Paris: Jacques du Puys, 1576.
3. Bradford, Anu. Digital Empires: The Global Battle to Regulate Technology. Oxford: Oxford University Press, 2023.
4. Bratton, Benjamin H. **The Stack: On Software and Sovereignty**. Cambridge, MA: MIT Press, 2016.
5. Couldry, Nick, and Ulises A. Mejias.**The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism**. Stanford, CA: Stanford University Press, 2019.
6. Crawford, Kate**. Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence**. New Haven, CT: Yale University Press, 2021.
7. Dunne, Tim, Milja Kurki, and Steve Smith, eds. **International Relations Theories: Discipline and Diversity.** 5th ed. Oxford: Oxford University Press, 2021.
8. Hobbes, Thomas. **Leviathan**. Edited by Richard Tuck. Cambridge: Cambridge University Press, 1996.
9. Keck, Margaret E., and Kathryn Sikkink. **Activists beyond Borders: Advocacy Networks in International Politics**. Ithaca, NY: Cornell University Press, 1998.
10. Krasner, Stephen D. **Sovereignty: Organized Hypocrisy**. Princeton, NJ: Princeton University Press, 1999.
11. Locke, John. **Two Treatises of Government**. Edited by Peter Laslett. Cambridge: Cambridge University Press, 1988.
12. Marwala, Tshilidzi. **Artificial Intelligence and Emerging Technologies in International Relations**. London: World Scientific, 2020.
13. Mejias, Ulises A., and Nick Couldry. **Data Grab: The New Colonialism of Big Tech and How to Fight Back**. London: Pluto Press, 2020.
14. Morgenthau, Hans J. **Politics Among Nations: The Struggle for Power and Peace**. 6th ed. New York: McGraw-Hill, 1985.
15. Ndzendze, Bhaso, and Tshilidzi Marwala. **Artificial Intelligence and International Relations Theories.** Cham: Springer, 2023.
16. Ning, Huansheng. **Cyberspace, Cyber Philosophy, and Cyberlogic: A Brief History of Cyberspace**. Boca Raton, FL: CRC Press, 2023.
17. Nye, Joseph S. Jr. **The Future of Power**. New York: PublicAffairs, 2011.
18. Pasquale, Frank. **The Black Box Society: The Secret Algorithms That Control Money and Information**. Cambridge, MA: Harvard University Press, 2015.
19. Radu, Roxana. **Steering the Governance of Artificial Intelligence: National Strategies in Perspective.** London: Policy and Society, 2021.
20. Rousseau, Jean-Jacques. **Du contrat social ou principes du droit politique**. Paris: Marc Michel Rey, 1762.
21. Schmitt, Carl. **Political Theology: Four Chapters on the Concept of Sovereignty**. Translated by George Schwab. Chicago: University of Chicago Press, 2005.

22. Steger, Manfred B. **Globalization: A Very Short Introduction**. 5th ed. Oxford: Oxford University Press, 2023.
23. Strange, Susan. **States and Markets**. 2nd ed. London: Pinter Publishers, 1994.
24. Strange, Susan.**The Retreat of the State: The Diffusion of Power in the World Economy.** Cambridge: Cambridge University Press, 1996.
25. Waltz, Kenneth N. **Theory of International Politics**. Reading, MA: Addison-Wesley, 1979.
26. Weber, Max. **From Max Weber: Essays in Sociology**. Translated and edited by H. H. Gerth and C. Wright Mills. New York: Oxford University Press, 1946.
27. Wendt, Alexander. **Social Theory of International Politics**. Cambridge: Cambridge University Press, 1999.
28. Zuboff, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. New York: PublicAffairs, 2019.

- **Articles in Academic Journals :**

1. Albous, Mohammad Rashed, Odeh Rashed Al-Jayyousi, and Melodena Stephens. "AI Governance in the GCC States: A Comparative Analysis of National AI Strategies." **Journal of Artificial Intelligence Research** 82 (2025): 2389–2422.
2. Aleeshan, P. M. A., M. N. P. Rifasha, and Mohamed Haniffa Mohamed Nairoos. "The Contribution of Medieval Muslims to the Development of Modern Science: A Review of Al Khwarizmi." **International Journal of Social Science and Economic Research** 8, no. 2 (February 2023): 215–230.
3. Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andrew Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et Matei Zaharia. "A View of Cloud Computing." **Communications of the ACM** 53, no. 4 (April 2010): 50–58.
4. Bendiek, Annegret, and Isabella Stuerzer. "The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate." **European Political Science Review** 15, no. 1 (January 23, 2023): 1–18.
5. Broeders, Dennis, Francesco Cristiano, and Marijn Kaminska. "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions." **Journal of European Public Policy** 30, no. 8 (2023): 1701–1724.
6. Broeders, Dennis, Arun Sukumar, Monica Kello, and Lise H. Andersen. "Digital Corporate Autonomy: Geo-economics and Corporate Agency in Conflict and Competition." **International Affairs** 100, no. 3 (2024): 112–134.
7. Buriaga, V. O., V. V. Djuzhoma, and E. A. Artemenko. "Shaping an Artificial Intelligence Regulatory Model: International and Domestic Experience." **Legal Issues in the Digital Age** 6, no. 2 (2025): 50–68.
8. Buruiană, A. "Black Box AI and the Sovereignty of Personal Data: Between GDPR and Digital Ethics." **European Journal of Law and Public Administration** 12, no. 1 (2025): 89–97.

9. Ceko, Elona. "The Global Role and Impact of the General Data Protection Regulation (GDPR): An International Comparative Approach." **Academicus International Scientific Journal** 29 (2024): 43–58.
10. Conti, Joseph A. "Supranational Stateness: International Courts and the Globalization of Political Power." **Michigan Journal of Law & Society** 1 (2007): 15–38.
11. Creemers, Rogier. "Cybersecurity Law and Regulation in China: Securing the Smart State." **China Law and Society Review** 6 (2021): 111–145.
12. Dahdal, Andrew Mazen, and Adel Abdel Ghafar. "The Digital Silk Road: 'Tech-Diplomacy' as a Paradigm for Understanding Technological Adoption and Emerging Digital Regulations in MENA." **Asian Journal of Law and Society** 12 (2025): 163–188.
13. Daskal, Jennifer. "The Un-Territoriality of Data." **Yale Law Journal** 125, no. 2 (2015): 326–398.
14. Dale, Robert. "Sovereign AI in 2025." Natural Language Processing 31 (2025): 1312–1321. Cambridge University Press.
15. Farrell, Henry, and Abraham L. Newman. "Cross-Network Weaponization in the Semiconductor Supply Chain." **International Studies Quarterly** 68, no. 1 (2024): 1–15.
16. Farell, Newman. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." **International Security** 44, no. 1 (2019): 42–79.
17. Florea, Adrian, and Reyko Huang. "Functional Sovereignty in Contested Territories." International Studies Quarterly 69, no. 2 (2025): 204–221.
18. Fratini, Samuele, Emmie Hine, Claudio Novelli, Huw Roberts, and Luciano Floridi. "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models." **Digital Society** 3, no. 1 (2024): 1–27.
19. Hulkó, Gábor, Judit Kálmán, and András Lapsánszky. "The Politics of Digital Sovereignty and the European Union's Legislation: Navigating Crises." **Frontiers in Political Science** 7 (2025): 45–61.
20. Kaya, M., and Hamza Shahid. "Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance." **Interdisciplinary Studies in Society, Law, and Politics** 4, no. 2 (2025): 219–233.
21. Malatji, Masike, and Alaa Tolah. "Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI."**AI and Ethics** 5 (2024): 883–895.
22. Neyland, Daniel, Véra Ehrenstein, and Sveta Milyaeva. "Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech**." Big Data & Society** 8, no. 2 (July–December 2021): 1–12.
23. Nizov, Vladimir A. "The Artificial Intelligence Influence on Structure of Power: Long-Term Transformation." **Legal Issues in the Digital Age** 6, no. 2 (2025): 183–212.
24. Olorunlana, Taiwo Justice. "Securing the Global Cloud: Addressing Data Sovereignty, Cross-Border Compliance, and Emerging Threats in a Decentralized World." **International Journal of Science, Architecture, Technology, and Environment** 2, no. 5 (May 2025): 1394–1407.

25. Petrella, Robert, Chris Miller, and Samuel Cooper. "Russia's Artificial Intelligence Strategy: The Role of State Owned Firms." **Orbis** 65, no. 1 (Winter 2021): 77–95.
26. Pierucci, Federico. "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace." **Digital Society** 4, no. 2 (2025). https://doi.org/10.1007/s44206-025-00189-4.
27. Pohle, Julia, and Thorsten Thiel. "Digital Sovereignty." Internet Policy Review 9, no. 4 (2020): 1–19.
28. Rao, R. "The Impact of Global Trade Agreements on National Sovereignty: A Legal Review." **Indian Journal of Law** 2, no. 5 (2024): 7–13.
29. Roberts, Huw, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, and Luciano Floridi. "Safeguarding European Values with Digital Sovereignty." **Nature Machine Intelligence** 3 (2021): 1030–1032.
30. Roberts, Huw, Emmanuel Kaula, Joshua Thomas, and Luciano Floridi. "The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation." **AI & Society** 36 (2021): 59–77.
31. Schindler, Sebastian, et al. "The Second Cold War: US–China Competition for Centrality in Infrastructure, Digital, Production, and Finance Networks." **Geopolitics** 28, no. 4 (August 2023): 1085–1112.
32. Sen, Sunanda, and Ria Chadha. "Data Localization: An Issue in the Cross-Border Digital Economy." **Indian Journal of Economics and Development** 17, no. 4 (2021): 1513–1520.
33. "The Rise of Techno-Geopolitical Uncertainty: Implications of the United States CHIPS and Science Act." **Journal of International Business Policy** 6, no. 2 (2023): 145–168. PMCID: PMC10066984.
34. Walter, Yoshija. "Managing the Race to the Moon: Global Policy and Governance in Artificial Intelligence Regulation—A Contemporary Overview and an Analysis of Socioeconomic Consequences." **Discover Artificial Intelligence** 4, no. 14 (2024). https://doi.org/10.1007/s44163-024-00109-4.
35. Xu, Jian. "Opening the 'Black Box' of Algorithms: Regulation of Algorithms in China**." Communication Research and Practice** 10, no. 3 (2024): 288–296.
36. Yevstratov, Yurii Ihorovych. "The History of Artificial Intelligence Development: From Antiquity to the Present." **Visnyk of Science and Education** 8, no. 38 (2025): 912–922.
37. Zou, Mimi, and Lu Zhang. "Navigating China's Regulatory Approach to Generative Artificial Intelligence and Large Language Models." **Cambridge Forum on AI: Law and Governance** 1, no. 1 (2024): 1–20.

- **Reports, Working Papers & Institutional Guides :**

1. Allison, Graham, Kevin Klyman, Karina Barbesino, and Hugo Yen. The Great Tech Rivalry: China vs. the U.S.Avoiding Great Power War Project. Cambridge, MA: **Belfer Center for Science and International Affairs**, Harvard Kennedy School, 2021.
2. African Union. Continental Artificial Intelligence Strategy for Africa. **Addis Ababa: African Union,** 2024.
3. Association of Southeast Asian Nations. ASEAN Guide on AI Governance and Ethics. Jakarta: **ASEAN Secretariat**, 2024.

4. Baezner, Marie, and Patrice Robin. Cyber Sovereignty and Data Sovereignty: Trend Analysis. Zürich: Center for Security Studies (CSS**), ETH Zürich, Risk and Resilience Team**, November 2018.
5. David Sacks, Emily Benson, "Balancing the Ledger: Export Controls on U.S. Chip Technology to China," **Center for Strategic and International Studies,** October 2024, Center for Strategic and International Studies CSIS.
6. Freitas, Marcus Vinícius De. Digital Sovereignty and Data Colonialism: Shaping a Just Digital Order for the Global South. Policy Paper No. 38/25. Rabat: **Policy Center for the New South**, 2025.
7. Fuller, Douglas B. Cutting Off Our Nose to Spite Our Face: US Policy toward China in Key Semiconductor Industry Inputs, Capital Equipment, and Electronic Design Automation Tools. Baltimore: Johns Hopkins University, **Social Science Research Network**, 2020.
8. Gineikyte-Kanclere, V., et al. European Software and Cyber Dependencies. Luxembourg: **European Parliament, Committee on Industry, Research and Energy, Policy Department for Transformation, Innovation and Health**, 2025.
9. Mayer, Maximilian, and Yen-Chi Lu. Digital Autonomy? Measuring the Global Digital Dependence Structure**.** SSRN Working Paper, no. 4404826. **Bonn: Center for Advanced Security, Strategic and Integration Studies** (CASSIS), 2022.
10. Organisation for Economic Co-operation and Development (OECD). A Preliminary Mapping of Data Localisation Measures. OECD Trade Policy Paper, no. 262. Paris: **OECD Publishing**, June 2022.
11. Panday, Jyoti, and Jeremy Malcolm. The Political Economy of Data Localization. Berlin: **ResearchGate Working Paper** Series, 2018.
12. Singh, S., and S. Sengupta. "Sovereign AI: Rethinking Autonomy in the Age of Global Interdependence." **arXiv preprint**, arXiv:2511.15734 (2025). https://doi.org/10.48550/arxiv.2511.15734.
13. Stanford Institute for Human-Centered Artificial Intelligence. AI Index Report 2026. **Stanford,**CA:StanfordUniversity,2026. https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf.
14. Yiyang Mei and Matthew Sag. The Illusory Normativity of Rights-Based AI Regulation**. arXiv preprint**, arXiv:2508.04122 (August 12, 2025).

- **Government Documents, Legislation & Executive Acts :**

1. Council of the European Union. Cyber Solidarity Act 2024: Strengthening EU Cybersecurity Capacities. ST 08047 EN 24. Brussels: **Council of the European Union**, 2024.
2. European Commission. Coordinated Plan on Artificial Intelligence: 2021 Review. Brussels: **European Commission**, December 15, 2021.
3. European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). **CELEX** 32024R1689. Eur-Lex, 2024.
4. State Council of the People's Republic of China. New Generation Artificial Intelligence Development Plan. Translated by DigiChina. **Stanford**, CA: Stanford University, July

20, 2017. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017.

5. Trump, Donald J. Ensuring a National Policy Framework for Artificial Intelligence. Executive Order, December 11, 2025.**The White House**. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy.
6. United Nations. Annex I: Global Digital Compact, Pact for the Future. **New York: United Nations**, 2024.
7. United States. National Cybersecurity Strategy. Washington, D.C.: **The White House**, March 2023.
8. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: **UNESCO**, 2021.
9. Vereinte Nationen. Governing AI for Humanity. New York/Geneva: **United Nations**, 2024.

- **Conference Papers**

1. María del Pilar Rodríguez Pita, Jorge Emiliano Pérez Martínez, and Alberto Urueña López. "From Concept to Method: A Framework for Measuring Digital Sovereignty." Paper presented at **the International Telecommunications Society** (ITS) 33rd European Conference: Digital Innovation and Transformation in Uncertain Times, Edinburgh, Scotland, June 29–July 1, 2025. Calgary: **International Telecommunications Society**, 2025.

- **Whitepapers, Digital Artifacts & Web Media:**

1. Analytics Vidhya. "Generative AI's Shift From GPT-3.5 to GPT-4 Journey." Analytics Vidhya Blog. Accessed May 2026.
2. Arab Reform Initiative. "AI in the National: AI Strategies of the Arab Region." Arab Reform Initiative, April 2025. https://www.arab-reform.net/publication/ai-in-the-national-ai-strategies-of-the-arab-region/.
3. Britannica Editors. "Semiconductor." Encyclopedia Britannica. Last modified May 5, 2026. https://www.britannica.com/science/semiconductor.
4. Cybercrime Diaries. "Russia's Sovereign RuNet – A Challenge to the Cybercrime Underworld?" Cybercrime Diaries Blog, April 18, 2026. https://www.cybercrimediaries.com/post/russia-s-sovereign-runet-a-challenge-to-the-cybercrime-underworld.
5. European Commission. "AI Act | Shaping Europe's Digital Future." Digital Economy and Society Portal. Accessed May 2026. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.
6. Georgetown Journal of International Affairs. "A Tool for Security? Cloud Computing in Border Control." March 17, 2026. https://gjia.georgetown.edu/2026/03/17/a-tool-for-security-cloud-computing-in-border-control.
7. Hosch, William L. "Machine Learning." Encyclopedia Britannica. Last modified January 12, 2026. https://www.britannica.com/technology/machine-learning.
8. Organisation for Economic Co-operation and Development (OECD). "The OECD AI Principles." OECD.AI Policy Observatory. Accessed May 2026. https://oecd.ai/en/ai-principles.

9. Shaikh, Jan Muhammad. “Maduro’s Capture: How the U.S. Redefined Power, Oil, and Sovereignty in Latin America.” The Friday Times, January 5, 2026. https://www.thefridaytimes.com/05-Jan-2026/u-s-seizes-nicol-s-maduro-daring-operation-triggering-regional-global-fallout.
10. Tabor, Nick. “Graphics Processing Unit (GPU).” Encyclopedia Britannica. Last modified May 2, 2026. https://www.britannica.com/technology/graphics-processing-unit.
11. Whitepaper. Risks with US Cloud. Cryptify Report, December 2025. https://cryptify.com/wp-content/uploads/2025/12/Whitepaper-Risks-with-US-cloud.pdf.