



National sovereignty in the face of the digital challenge: Who controls the internet? Is our privacy protected and guaranteed?

Nabila Addane 

Faculty of Information and Communication Sciences

University of Algiers 3 (Algeria)

addane.nabila@univ-alger3.dz

 <https://orcid.org/0000-0002-5194-3100>

Received: 22/11/2025

Accepted: 28/01/2026

Abstract:

The world is witnessing a fundamental shift in the concept of national sovereignty. Faced with the unprecedentedly rapid and escalating digital challenge, national sovereignty, in its classical sense based on the monopoly of power within defined geographical boundaries, is no longer sufficient to understand the balance of power in the digital age. We are now confronted with a new and profound sovereignty gap that has gradually stripped the state of its control over cyberspace. The struggle for governance and power is now a three-way contest between nation-states, transnational technology companies, and the global tech community. This struggle has reduced state sovereignty to an attempt to control it through digital walls and data localization legislation.

Therefore, this study seeks to explore the implications of national sovereignty in the digital age, and the fate of our data and privacy. We question whether our data has become a commodity or remains protected, and who truly controls the lifeblood of modern civilization. Where does our privacy stand amidst this battle?

Keywords: Digital space ,digital sovereignty, ,National sovereignty International actors, privacy

I. INTRODUCTION

Thinkers, starting with the Renaissance and Enlightenment, have long been interested in the concept of sovereignty following conflicts and the imbalance of power between European states. Sovereignty was considered a fundamental principle for the establishment and continuation of the state, or rather, for the restoration of its prestige. It is a central condition for its existence and, with its demise, its disappearance. Faced with these conditions, attempts continued to crystallize ideas and theories, but the digital age had a different opinion. We are now facing a qualitative shift that has taken us from the abstract to the digital, and from traditional sovereignty to digital sovereignty. The use of technology has grown, casting its shadows, particularly the negative ones, on all countries, especially those in the developing world. Threats have become palpable within their borders with the click of a button, and the state has transformed from the sole actor on the scene to the emergence of other actors competing with the state for its sovereignty, particularly with regard to data protection and privacy preservation.

From this perspective, this study aims to analyze the nature of the challenge posed by cyberspace to the concept of traditional national sovereignty, examine the balance of power in controlling the global network, and assess the extent of individual privacy protection amid this conflict. This study concludes that sovereignty has not disappeared, but rather has transformed from absolute sovereignty to "negotiated sovereignty," whereby states are forced to negotiate and engage with new actors, such as transnational technology companies. Privacy, on the other hand, has become a victim of this conflict, being violated by states under the pretext of national security and by companies motivated by profit, placing individuals in a vulnerable position requiring more effective legal protection

The Importance of the Research

This research is critically important for several reasons:

- ✚ It contributes to modern political and legal theory by updating the centuries-old concept of sovereignty for the 21st century. It provides a new framework to understand power dynamics in a globalized, digital world.
- ✚ It highlights a pressing societal issue—the erosion of privacy, by diagnosing privacy as a "victim" of this power struggle, the research underscores the urgent need for more robust and effective legal protections for individuals, making it a crucial work for human rights advocacy and legal reform.
- ✚ It specifically acknowledges the disproportionate impact of these changes on developing countries, which often have less capacity to resist digital threats or negotiate with powerful tech corporations. This makes the research relevant for international development and global digital governance discussions.

Research Problematic

The core problem of this research addresses the fundamental tension between the traditional, Westphalian concept of state sovereignty and the new realities of the digital age. Cyberspace, by its borderless and decentralized nature, challenges the state's historical monopoly on power, regulation, and territorial control. This creates a triple crisis:

- ✓ **A Crisis of Control:** The state is no longer the only actor, as powerful transnational technology corporations now wield significant influence, often rivaling or surpassing that of states, particularly in areas like data control and network infrastructure.
- ✓ **A Crisis of Security:** Digital threats can penetrate national borders "with the click of a button," making traditional national security paradigms inadequate and forcing states to react in ways that often infringe on individual rights.
- ✓ **A Crisis of Rights:** The individual's right to privacy is caught in the crossfire, being

eroded by states in the name of national security and by corporations in the pursuit of profit, leaving individuals vulnerable.

The central problematic of this study is: **How has cyberspace changed the traditional concept of national sovereignty and opened the way for other actors to compete with the state in its control and affect the balance of power and the protection of individual privacy?**

Research Objectives

This study aims to achieve the following specific objectives:

- To analyze the nature of the challenge that cyberspace poses to the traditional, abstract concept of national sovereignty.
- To examine the shifting balance of power in the control of the global digital network, focusing on the new dynamic between nation-states and non-state actors (especially transnational tech corporations).
- To assess the extent of individual privacy protection within this new conflict, identifying the specific threats posed by both state and corporate actors.

1. National sovereignty: from geographical borders to moral authority, and from national to the international level

Jean Bodin is considered the "father" of the modern use of the concept of "sovereignty." It is the fundamental characteristic of the state, appearing within it and disappearing with its demise. Bodin participated in the "first systematic discussion of the nature" of the concept through his work "The Six Books of the Republic," where he defines it as **"the absolute and permanent power in the republic."** What is noticeable about the above definition is its focus on the internal model of the local power hierarchy by placing sovereignty at the top. In other words, sovereignty is viewed as "the highest authority in the hierarchical organizational structure of society, that is, the highest unified authority." (Chander &Sun, 2023, p214)

While the definition provides a good explanation of sovereignty in the local context, it may encounter some complications at the international level. All states are considered to be equally sovereign in principle, but in reality, states differ in their relative powers depending on their military or economic strength.

In this regard, Eimer de Vattel offered a solution, shifting the concept of sovereignty from the national to the international level, and from the internal to the external dimension, by defining sovereignty as **"exclusive authority from outside."** That is, it is **"a political body that represents the people alone externally and is not subject to any foreign state or any external higher law."** By focusing on this "integrated independent authority," Vattel laid the foundation for the discourse on sovereignty under international law, which is based on the fundamental concept of states as independent actors. (Chander &Sun, 2023, p215)

The discussions did not stop there, but gradually escalated, taking the term to other, more complex levels, such as the ethical dimension. Many scholars have addressed this point in a similar vein. In his article **Bellamy** illustrates the different connotations of sovereignty, starting with Pre-Sovereignty which describes a theoretical or historical condition before the emergence of the modern notion of sovereignty, characterized by a situation where there was no single, centralized sovereign authority recognized across a political community. Instead, political power was more dispersed, often rooted in customary or tribal arrangements, or based on overlapping authorities without a clear, singular sovereign. The pre-sovereignty model emphasizes a state of polity where the social and political ordering is based on

decentralized or traditional norms rather than a centralized sovereign entity (Bellamy, 2003).

After that, the concept of sovereignty is emerged and multifaceted and can be understood in various ways depending on the context. **Kahn Clea and Andrew Cunningham**, in their article, identified these meanings, which include complex interpretations of the concept and its fundamental meanings, as follows (Clea, Cunningham, 2013):

- **Traditional/Westphalian Sovereignty:** This refers to each state possessing supreme authority over its territory and internal affairs, free from any external interference. This sovereignty is embodied in the principles of non-intervention and equality among states, as stipulated in the Treaty of Westphalia.
- **Internal Sovereignty:** This is the exclusive authority of the state to manage its internal affairs, including legislation, law enforcement, and resource management, without any external influence from any other state or entity.
- **External Sovereignty:** This encompasses the recognition of the state's independence and equal standing within the international system, enabling it to conclude treaties with other states and establish international relations. Sovereignty as competence or responsibility: This is the most modern interpretation, emphasizing the state's ability to provide protection and services to its population. This view of sovereignty links the state's competence and duty to protect its citizens, as manifested in the principle of the responsibility to protect.
- **Sovereignty as legitimacy:** This refers to the moral and political authority of the state to govern, which is often linked to its ability to maintain order and provide for the needs of its people.

What can be generally concluded from the preceding definitions presented for constructing a comprehensive framework for the concept of sovereignty is its continuous evolution, based primarily on accumulation rather than radical rupture. It is evident from the authors' definitions that the concept has shifted from a rigid notion of absolute control over internal affairs to a more nuanced understanding encompassing the responsibilities of the state and its role in the international community as a whole.

Furthermore, adding an ethical dimension to the meaning of state sovereignty essentially signifies the responsibilities incumbent upon the state to achieve the common good for its citizens and its responsibility towards the international community. Here, we have moved from concepts that focus on natural geographical boundaries when defining state authority and control over its territory to concepts that are not so much constrained by borders as by the ethical responsibility imposed by the concept. This ethical responsibility has resulted from environmental and technological changes at all levels, accompanied by a growing awareness among citizens who have realized that protecting borders is insufficient to guarantee human security, especially when technology threatens them with the click of a button.

2. The paradox of New sovereignty

While the term "digital sovereignty" has been widely adopted by nations, it was presented sometimes as an alternative and at other times as a reinforcement of traditional sovereignty, but the matter became serious and the concept became an inevitability and a necessary response to the challenges of cyberspace, its practical implementation reveals a fundamental contradiction. States assert their sovereignty in the digital realm through laws and regulations, yet they are simultaneously compelled to rely on the very transnational corporate infrastructure and architectures that undermine that sovereignty. This creates a problematic defined by a cycle of dependency and assertion:

1. **The Infrastructure Dilemma:** The foundational layers of the digital world—cloud computing, submarine cables, satellite networks, operating systems, and major software platforms—are predominantly owned and controlled by a handful of private, transnational corporations (e.g., Amazon, Google, Microsoft, Meta). For a state to be "present" and functional in the digital age, it must, by necessity, utilize these infrastructures. This creates a structural dependency that inherently limits true sovereign control.
2. **The Regulatory Paradox:** In an attempt to reassert control, states enact national laws on data localization, content moderation, and digital taxation. However, these regulatory actions are not exercising of absolute sovereignty but are, in fact, negotiations. They are demands made upon external corporate actors who control the platform. The enforcement of these laws often requires complex international legal battles and compliance negotiations with these very corporations, reinforcing the concept of "negotiated sovereignty" not as a choice, but as an imposed condition.
3. **The Security Compromise:** The pursuit of national security in cyberspace further illustrates this paradox. To defend against digital threats, states develop advanced capabilities. However, they also increasingly depend on threat intelligence and security services from the private sector. Furthermore, their own surveillance measures for security purposes often mirror the data-collection practices of corporations they seek to regulate, blurring the lines between protector and violator and deepening the crisis for individual privacy.

At this stage different concepts discuss the changing world of digital age at several levels, which skip from the physical borders and turn the attention to intangible aspects of sovereignty, rather than:

a. Technological sovereignty

"Technological sovereignty" focuses on developing local technologies in key areas. This is exemplified by the European Commission's 2020 publication of three important strategic documents: "Shaping the Digital Future of Europe," the "White Paper on Artificial Intelligence," and the "European Data Strategy." The aim was to reclaim "technological sovereignty" and strengthen the EU's responsibility in developing and setting standards for cutting-edge technologies and applications, such as artificial intelligence, big data, and 5G. (The World Internet Conference, 2024)

b. Digital sovereignty

Digital sovereignty refers to the effort by nations to control their digital infrastructure, data, and technological capabilities to ensure autonomy, security, and economic independence in the digital realm. It involves implementing regulatory frameworks, data localization policies, and resilient infrastructure to reduce reliance on foreign technology and mitigate vulnerabilities to external threats and monopolistic practices. This concept is shaped by regional differences, with China emphasizing a culturally and politically informed approach, including mass surveillance, while Western countries prioritize privacy, cybersecurity, and free market principles, leading to increased regulation and control measures. (Thorsten, 2023, Pp 40-46)

Overall, digital sovereignty seeks to balance global connectivity with national strategic interests through policies such as data localization, industrial policy, and legal regulations, aiming to safeguard sovereignty in the face of digital globalization.

"Digital sovereignty" aims to enhance "strategic autonomy." The European Parliament defined "digital sovereignty" in 2020 as "Europe's ability to operate autonomously in the digital world, and it should be understood in terms of both protective mechanisms and offensive tools to promote digital innovation (including collaboration with companies outside the EU)." This concept was put forward to maintain the EU's independence, competitiveness, and leadership in the face of competition in the digital world, emphasizing the ability of countries to drive their own digital development. (The World Internet Conference, 2024)

c. Data Sovereignty,

At first, many considered the idea of data sovereignty as an oxymoron, since data naturally crosses borders while sovereignty is usually tied to a specific portion. This makes things more complicated when it comes to creating, processing, storing, and sharing data. As a result, definitions of the term have often focused either on the ethical side, like data ownership and personal control, or the technical side, such as connecting the validity of stored data to its physical location in the cloud.

Data sovereignty refers to "purposeful control, ownership, and other claims to data or its infrastructure." This emphasis on control and authority aligns with the traditional notions of sovereignty discussed earlier in this study. To narrow our focus, we can define data sovereignty as "an independent supreme authority over data trade, capable of setting rules and exceptions, particularly with regard to, firstly, border measures such as the transfer of data across borders; and secondly, local regulations such as data localization requirements." The principle of data sovereignty holds that "data about an individual belongs to them, and they should remain in control of how and for what purpose that data is used." (Chander & Sun, 2023, Pp 216-217).

While the concepts mentioned above may differ in their objectives or focus, they are inherently interconnected. Relevant practices and studies have demonstrated the significance and scope of sovereignty in cyberspace.

3. Digital space :beyond the truth

Cyberspace is essentially a virtual space, enabling instant communication with little regard for physical distance. In his article on Cyberspace, **Daniel Lambach** discusses ideas that render cyberspace ungovernable and ungovernable. As evidence, he cites the famous "Declaration of Independence of Cyberspace," in which John Perry Barlow warned world governments: "On behalf of the future, I ask you, relics of the past, to leave us alone. You are not welcome among us. You have no sovereignty where we gather." According to this view, cyberspace is "no man's land where social relations and laws have no historical existence and must be reinvented." Faced with this reality, we now live in "Internet exceptionalism," where experimental developments have solidified the notion of the internet's ungovernability. Cyberspace can no longer be conceived as separate from the "real world." States assert their authority over cyberspace by translating familiar territorial logic into this "uncharted territory" (Newland, as former German Chancellor Angela Merkel once called it), where, on the one hand, corporations create geographic zones through registration requirements and limitations on interoperability between "internet ecosystems." On the other hand, private users and creators establish virtual zones in online communities, social media, or closed chat groups (Lambach, 2019).

At this stage, which threw the digital space with its burden on national sovereignty, the meanings changed not only in words but in practices and attitudes, a new connotation is shown called Post-Sovereignty, according to Bellamy this concept refers to a conceptual stage or condition in which the traditional notion of absolute, centralized, and uncontested sovereign authority is diminished or undermined. It emphasizes the weakening or dispersal of sovereign power due to processes such as globalization, international organizations, and transnational rights frameworks. In this model, sovereignty is no longer primarily held by individual states or God-given, but is shared, limited, or transformed, leading to a political condition where the authority of states is constrained or redistributed across multiple actors and norms (Bellamy, 2003).

After the flourish of new concepts as well as **information sovereignty, technological sovereignty, data sovereignty, digital sovereignty**... researchers called for a varied meaning it was called **Mixed Sovereignty** which is a conceptual framework that combines elements of sovereignty and pre-sovereignty, advocating a system where sovereign power is divided, shared, or balanced among different institutions, norms, and actors. Rather than a monolithic, absolute sovereignty residing solely with the state or ruler, mixed sovereignty involves a layering or distribution of authority that includes legal, political, and normative sources. It aims to provide a more nuanced, pluralistic understanding of sovereignty that recognizes its complexity and often its contested nature in practice (Bellamy, 2003).

4. The Impact of Internet & Digital Space on Our Privacy: Since when Did creating an account become an attestation to data sharing?

Globalization has increased social differentiation, have enhanced interconnectedness at the international level, and simultaneously produced greater heterogeneity at regional and local levels. These forces have diminished states' capacity to independently formulate socio-economic, foreign, and defense policies, and have complicated the construction of a unified national identity that could sustain allegiance to the state and its institutions. As a result, citizens increasingly question not only the functional competence of states to ensure their security but also the legitimacy of democratic states to define and restrict their rights.

This gap has widened considerably, especially with the rise of the internet, which has undermined, to some extent, the authority of the state, which has come under scrutiny, and voices demanding transparency have grown. In the face of these transformations, the use of the internet has expanded and become a weapon in an increasingly widespread information war, that is growing and spreading on all levels, as happened, for example, in the American elections of 2016, where the political discussions that emerged through digital platforms such as Twitter were issued by automated accounts, and the same method was used in Mexico to counter criticisms directed at the government. (Hemsley and all, 2018, p 01)

The term "**click wrap**" was introduced as a digital tool that facilitates consent processes by giving users the opportunity to quickly accept or reject digital media policies. This click wrap has become the dominant form of consent to the terms of digital platforms that a person might encounter and click on when creating an account. Attention is diverted from policies related to privacy and reputation protection, thus normalizing the circumvention of legal consent terms. This gives the companies controlling these digital platforms, such as social media platforms, legal rights to user data in ways that users are largely unaware of. (Hemsley and all, 2018, p 02)

Many of us have encountered such notices and materials at least once while using these applications. We might skim over them, even though our data and privacy are inextricably linked to them. This is what companies do because they know that today's user is so busy and stressed that they are unable to read the materials protecting their privacy. They skip them without realizing that they are granting the companies the right to infringe upon their data and privacy. This happens frequently when these platforms publish updates that may seem innocuous on the surface but contain blatant violations of privacy, as happened, for example... Snapchat and Instagram updates include features that allow artificial intelligence to use and share your data, often with the user's unwitting consent. This data may have been part of content the user has approved without scrutinizing its content.

Similarly, and similar to a feature introduced by Google, when you create any personal or professional account on their platform, you are agreeing to Google sharing your data and photos with artificial intelligence. This poses a blatant challenge to the privacy and data protection that these companies are supposed to provide. We have also recently witnessed the global trend of reuniting your childhood self with your adult self, dubbed "embracing your inner child." What this trend conceals is that the most popular app used for this purpose, Gemini, retains all your data and photos that you have shared with it and uses them to train artificial intelligence, granting it permission to share them as well. This is the danger that threatens our safety.

In the midst of these developments, another challenge has emerged concerning the scientific aspects, which revolves around the concept of **Pseudoknowledge** to describe false narratives that have become accepted in society as a plausible reality. Is the fake knowledge that has flourished via the Internet a dynamic built by actors over time, given that individuals create credibility by reinterpreting a wide range of electronic sources, including some academic sources, to support, defend, and refine the narrative when attacked? Therefore, suppressing fake knowledge on the Internet, especially academic fake knowledge, will remain a serious challenge (Hemsley and all, 2018, p 02)

Giant tech companies have emerged as key players, controlling digital infrastructure and shaping human behavior through their platforms. In response, countries are striving to regain control through digital walls and data localization legislation, while the traditional model based on global governance struggles to survive.

A significant shift in the mechanisms of the digital space is the introduction of satellite-based cyberspace, which facilitates bypassing censorship and access control by national governments, thus putting their national sovereignty at risk. This is especially true given the growing voices expressing concern about a blatant violation of national sovereignty in the information age. While some argue that this concern can be counterbalanced by the legal and material capacity of national governments to license and shut down internet service providers and control physical infrastructure, another development—the transfer of cyber infrastructure from Earth to space—necessitates ground-based control centers that can be distributed globally, making it easier for national governments to circumvent control. This is particularly relevant when multinational space companies provide internet satellites that can operate simultaneously in multiple countries. Indeed, some argue that a major factor behind the development of satellite-based cyberspace is that many countries have made legal changes enabling private space projects. Luxembourg, a small European country, has, over the past 10 to 15 years, made public and private space programs a key national strategy, particularly concerning satellites undertaken by multinational corporations (Dunn Cavelty&Wenger,2022).

The study presented by **Mueller** points to growing concern about the potential fragmentation of the internet. When states assert their sovereignty over this domain, they

often aim to control or regulate the flow of information within their borders, leading to calls for “digital borders” or separate national networks. These claims threaten the idea of a unified and open internet and risk a fragmentation process in which cyberspace is divided into isolated or incompatible national sectors. Asserting sovereignty in cyberspace—such as control over data, content, or infrastructure—can create barriers that weaken the internet’s interconnectedness and openness. Efforts to impose sovereignty in cyberspace may also lead to a fragmented internet, with separate national or regional “networks,” rather than a cohesive global network. The author argues that recognizing cyberspace as a shared global domain offers a better path to maintaining interconnectedness and avoiding this fragmentation. (Müller 2019, Pp 08-14).

5. National sovereignty in the face of digital challenge: the emergence of new actors

Sovereignty has not disappeared entirely. While states still retain the ability to withdraw from international arrangements or choose their levels of compliance, their actual sovereignty has been significantly weakened and its nature altered. States are increasingly obligated to negotiate with other states and international organizations, recognize the authority of international courts, and operate within complex networks of transnational norms—factors that challenge the traditional centralized model of sovereignty. (Bellamy, 2003).

In essence, globalization diffuses, constrains, and transforms sovereignty, moving away from the idea of states as absolute and self-contained entities toward a more interconnected and norm-based system where sovereignty is shared or tiered rather than monopolized (Bellamy, 2003).

The impact of globalization on state sovereignty as a process that challenges and alters traditional notions of sovereign power. Globalization has increased the interdependence between states and non-state actors, making it more difficult for states to maintain independent control over their domestic and international policies. This interdependence reinforces international legal and regulatory frameworks which, while protecting fundamental rights such as free trade, often disadvantage poorer states and weaken their unilateral capacity to control economic and social affairs.(Bellamy, 2003).

Furthermore, globalization introduces mechanisms—such as international courts, regulatory bodies, and intergovernmental organizations—that impose limitations on state sovereignty, reducing its absolute and singular control. Consequently, sovereignty is perceived as more fluid and less absolute, as states recognize the legal authority exercised by various international bodies, which in turn diminishes their traditional capacity for independent, final decision-making.(Bellamy, 2003).

In the same point, giant technology companies pose a formidable challenge to national governments in terms of the powers they wield. In this sense, it could be argued that digital companies possess powers comparable to those of traditional sovereign entities. This led **Lawrence Lessig** to expand the concept of sovereignty by equating it with "control." He developed two models of sovereignty based on who holds control. The first model focused on "citizen sovereignty," which deals with institutions such as universities and social clubs, etc., that "give consumers control over the rules that will govern them." On the other hand, in the "merchant sovereignty" model, rules are imposed by merchants and are not chosen by consumers. These rules are based on "take it or leave it." (Chander &Sun, 2023, Pp 216-217)

Regarding who controls data and how the digital age has impacted privacy, the study on data sovereignty identified three main groups of actors (players): the individual, who provides raw data and uses processed data; the company, which processes raw input from the consumer

and typically controls that data; and the state, which monitors and regulates data use by the first two groups. Their differing interests often lead to conflicting priorities, with the individual advocating for privacy protection, the company promoting unimpeded data flow, and the state focusing on security implications. Disagreements among these three groups often result in various restrictive measures, the most common being restrictions on cross-border data flows in the name of protecting individual privacy or national security. (Chander & Sun, 2023, p218)

The problem of multiple international actors that can influence national sovereignty—and may even direct and exert pressure on it—poses numerous challenges at all levels, such as:

- ✓ The economic challenge: The dominance of data-driven business models and tax evasion by multinational corporations undermines the state's ability to monitor and thus limits the scope of state intervention, placing sovereignty between the hammer and anvil of multinational corporations.
- ✓ The legal challenge: Judicial disputes (such as the dispute between the European Union and the United States regarding citizens' data) highlight the role of legal regulations in achieving stability and balance between the authority of the state as the highest authority and the power of multinational corporations. This is what the European Union has sought to achieve through regulations that redistribute power and prioritize domestic laws over those that corporations seek to implement.
- ✓ The security challenge: The use of cyberspace to launch attacks between states (hacking and hybrid warfare) violates sovereignty. As has been acknowledged, the digital space has opened the door for a state's borders to be threatened with the click of a button. A single click can blatantly violate a state's sovereignty and leak its citizens' data, thus violating its rights. Their privacy, which is supposed to be protected and guaranteed, and we have many examples in history regarding these issues. Therefore, the multiplicity of actors will either rearrange the balance of power or destroy it in a way that can never be repaired.

While all countries agree on the need to balance the conflicting interests of various stakeholders, their approaches often differ in practice. Some jurisdictions prioritize the need to protect user privacy. A good example is the European Union's General Data Protection Regulation (GDPR), which recognizes the "protection of natural persons with regard to the processing of personal data" as a "fundamental right." On the other hand, some jurisdictions prioritize the commercial interests of companies. For example, in the United States, the Communications Act of 1996 states that "the policy of the United States...is to maintain...the free market...without restrictions from federal or state regulations." In contrast, national security concerns are often cited to justify restrictions on cross-border data flows, albeit to varying degrees in different countries. A recent example is China's Cybersecurity Law of 2017, which imposes multiple restrictions aimed at "protecting cybersecurity, safeguarding the sovereignty of cyberspace, and national security." (Chander & Sun, 2023, p220)

Conclusion

In the end we can conclude that National sovereignty in this age characterized by digital transformation, is a contemporary era increasingly characterized by its hybrid nature, where the traditional monopoly of the state over authority is shared and contested by a range of actors beyond the state itself. This includes private contractors, multinational corporations, and non-governmental organizations that operate alongside or within state frameworks, creating complex public-private relationships that transcend conventional territorial boundaries.

Furthermore, transnational governance mechanisms and international legal institutions

contribute to reshaping sovereignty by introducing norms and adjudications that challenge exclusive state control. The rise of local political actors empowered by globalization and digital communication networks further complicates sovereignty by integrating subnational voices into global political processes. Additionally, semi-state actors in cybersecurity and environmental governance illustrate how sovereignty is negotiated amid overlapping jurisdictions and interests. Collectively, these dynamics demonstrate that national sovereignty is a fluid and evolving concept, continuously redefined through multifaceted interactions within the global order.

Results:

From the study we can conclude the following key findings as:

- **The Erosion of the State's Monopoly:** The Westphalian model of absolute state authority within its borders is no longer tenable. The state is no longer the sole, dominant actor.
- **The Rise of Hybrid Authority:** Sovereignty is now "shared and contested" by a diverse set of non-state actors:
- **Private Sector:** Multinational corporations (e.g., in tech, finance) and private contractors (e.g., in military and security).
- **Transnational Bodies:** International courts, regulatory organizations, and standard-setting bodies.
- **Sub-state and Local Actors:** Cities and regions that engage directly in global diplomacy (e.g., on climate change).
- **Semi-state Actors:** Entities that operate in a grey area between public and private, especially in domains like cybersecurity.
- **The Blurring of Boundaries:** The traditional inside/outside distinction of sovereignty is breaking down due to "complex public-private relationships" that "transcend conventional territorial boundaries."
- **Sovereignty as a Negotiated Process:** The final result is that sovereignty is no longer a static condition but a fluid and evolving concept. It is continuously being "redefined through multifaceted interactions" and must be "negotiated."

Recommendations:

Based on the results, a state that wishes to protect and project its sovereignty effectively must adapt its strategies. Here are the key recommendations:

- ✓ **Develop Regulatory and Legal Agility:** Outdated legal frameworks leave a state vulnerable. Agility allows a state to assert its authority in new domains effectively by Updating domestic laws and regulations to keep pace with digital, economic, and security challenges. This includes creating robust data protection laws, regulations for AI and cyber operations, and legal frameworks for dealing with semi-state and non-state actors.
- ✓ **Invest in "Sovereignty Capabilities:** Sovereignty must be actively maintained and

defended in these new arenas where it is most contested, by Building state capacity in critical, modern domains, particularly:

- Cybersecurity: Develop robust national cybersecurity institutions and a skilled workforce to defend against state and non-state actors.
 - Digital Infrastructure: Control and secure critical digital infrastructure.
 - Strategic Communication: Combat disinformation and shape the global narrative.
- ✓ Foster Domestic Legitimacy and Inclusivity: A state whose internal sovereignty is contested by empowered sub-state actors is weaker on the global stage. Internal cohesion and legitimacy are the foundation for effective external sovereignty. Acknowledge and manage the "rise of local political actors." Create formal and informal channels for subnational voices to contribute to national positions on global issues.
 - ✓ Clarify the Role of Public-Private Partnerships (PPPs) This prevents the state from ceding its essential authority and ensures that private partners remain accountable to public goals, by Developing clear doctrines, contracts, and oversight mechanisms for engaging with private contractors and corporations, especially in sensitive areas like security and data management.
 - ✓ Engage Proactively in Transnational Governance: If state is not at the table setting the rules, you will be on the menu, forced to abide by rules others have created, and by participating vigorously in international forums setting standards for digital trade, AI ethics, and environmental policy.

In general, states must transition from being fortress-like sovereigns to being agile, networked managers of sovereignty. The goal is no longer to exclude external influence but to manage it intelligently and project influence effectively within a crowded and complex global ecosystem.

– **Referrals and references:**

- Anupam Chander, Sun Haochen (2023), *Data Sovereignty from the Digital Silk Road to the Return of the State*, Oxford University Press, New York;
- Bellamy, R. (2003). Sovereignty, post- Sovereignty, and pre- Sovereignty: three Models of the state, democracy and rights within the EU. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.1530445>
- Dunn Cavelty, M., Wenger, A., (2022), *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, 1st Published, Routledge, New York;
- Hemsley, J., Jacobson, J., Gruzd, A., & Mai, P. (2018). Social Media for Social Good or Evil: An Introduction. *Social Media + Society*, 4(3). <https://doi.org/10.1177/2056305118786719>
- Kahn, Clea, and Andrew Cunningham. "Introduction to the issue of state sovereignty and humanitarian action." *Disasters* vol. 37, 2013, pp. 147–154.
- Lambach, D.,(2019), *The Territorialization of Cyberspace*, *International Studies Review* 0, 1–25;
- Mueller, M. L. (2019). Against sovereignty in cyberspace. *International Studies Review*. <https://doi.org/10.1093/isr/viz044>
- The World Internet Conference (2024), *Sovereignty in Cyberspace: Theory and Practice (Version 4.0)*, available on: https://www.wicinternet.org/2024-01/16/c_956165.htm , consulted on 15/10/2025.
- Thorsten, J. (2023). *The Digital sovereignty Trap: Avoiding the Return of silos and divided world*. Springer Briefs in International Relations.