International Journal of Multidisciplinary Research Updates

Journal homepage: https://orionjournals.com/ijmru/

ISSN: 2783-0179 (Online)

(RESEARCH ARTICLE)

Check for updates

Digital sovereignty in an era of cyber threats and global connectivity

Jin young Hwang *

University of Edinburgh MA Social Policy and Economics, United Kingdom.

International Journal of Multidisciplinary Research Updates, 2025, 09(02), 012-023

Publication history: Received on 14 March 2025; revised on 22 April 2025; accepted on 25 April 2025

Article DOI: https://doi.org/10.53430/ijmru.2025.9.2.0023

Abstract

Digital sovereignty is significant in the 21st century because of increased threats to cyber security and increased level of connectivity. This research investigates the dilemma of the states and their quest for mastering information technologies, and creating and maintaining their sovereign digital space while being a part of the digital global network. These aspects of the interactions between international law and cyberspace are explored through doctrinal assessment of legal instruments and case-study approaches to issues touching on data localization laws, cybersecurity threats and the roles of non-state actors – such as multinational corporations and international organizations. It analyses and assesses the legal measures that states use in exercising digital control, regulate cross border data flows for security reasons, and in the international agreements and national laws' application. The research reveals the conflict between state-centered and global collaborations approaches and provides ideas for the coordination of the cybersecurity regulations around the world, to enhance communication between states and the non-state players, and to maintain the stability of good governance. Specifically, this work advances important knowledge regarding the state of digital governance and presents approaches to safeguard digital sovereignty together with envisioning a new age of innovation and collaboration in cyberspace.

Keywords: Digital Sovereignty; Cybersecurity; Data Localization; Global Connectivity; International Governance; And Non-State Actors

1 Introduction

The concept of digital sovereignty has emerged as a critical focal point in the 21st century, driven by the escalating risks posed by cyber threats and the complexities of global connectivity. Digital sovereignty refers to the idea that states should have control over the digital infrastructure and data within their borders, allowing them to protect their citizens, regulate their economies, and safeguard their national security interests (Wu, 2021). The rise of digital technologies, particularly the Internet, has interconnected the world in ways that have transcended traditional borders, creating opportunities for economic growth, cultural exchange, and innovation. However, these advancements have also introduced a new landscape of risks, including data security threats, cyberattacks, and the weaponization of information.

The balance between national control over digital infrastructure and active participation in a globally interconnected Internet has become a primary challenge. On one hand, states have an inherent interest in controlling the flow of data and securing their digital spaces against external threats (Wu, 2021). On the other hand, they are increasingly reliant on global digital platforms, multinational companies, and international data exchanges that make national regulation more difficult to enforce. This tension creates a paradox, as countries seek to exert control over their digital spaces without stifling innovation or their ability to participate in the global digital economy (Mathur, n.d.).

* Corresponding author: Jin young Hwang.

Key challenges to digital sovereignty include issues surrounding data security and privacy, transnational data flows, cybersecurity, and the growing influence of powerful non-state actors. The global nature of the internet complicates the enforcement of national laws and regulations, as data often crosses borders in ways that defy traditional state-based legal structures (Mueller, 2020). Cybersecurity threats, such as hacking, data breaches, and cyber warfare, have become increasingly sophisticated, and states must grapple with how to protect their citizens from these evolving risks. Additionally, geopolitical power struggles are emerging as states seek to influence or control key aspects of global digital infrastructure, such as data centers, cloud computing, and 5G networks.

In response to these challenges, countries are adopting various legal and policy measures aimed at protecting their digital sovereignty. These include data localization laws, which require that data generated within a country's borders be stored and processed domestically, as well as national cybersecurity strategies aimed at fortifying digital infrastructure (Perritt, 1997). At the same time, many states are participating in international digital governance frameworks, seeking to balance national interests with the need for global cooperation. This complex interplay between national regulation and global digital integration forms the backdrop of this research.

1.1 Research Problem and Rationale

States face increasing pressure to safeguard their digital sovereignty while engaging in the global digital ecosystem. As digital threats grow in scale and sophistication, governments are under mounting pressure to protect critical national infrastructure from cyberattacks, ensure the security of their citizens' data, and maintain control over the economic and social dimensions of the digital age (Gur, 2022). However, this goal must be balanced with the reality of an interconnected world in which digital technologies transcend national borders, and where global actors, such as multinational corporations and international organizations, wield significant influence.

The challenge for states lies in navigating this balance—ensuring robust national protections against cyber threats and data breaches while also participating in international efforts to govern the digital domain. This includes coordinating efforts with other states and multinational bodies to address issues such as data privacy, cross-border data flows, and cybercrime. The complexity of this issue is compounded by geopolitical power struggles over the control of digital infrastructure, the internet's governance, and the regulatory frameworks that shape digital commerce and security. As digital threats evolve, so too must the frameworks that govern them (Pohle & Thiel, 2020).

This research aims to explore the strategies employed by states to assert their digital sovereignty while managing the challenges and opportunities presented by global connectivity. Understanding how states navigate the complexities of digital sovereignty is essential for grasping the future of international digital governance, cybersecurity policies, and the international cooperation required to address the cross-border nature of digital threats (Fauzi et al., 2024). The research will provide valuable insights into the ways states can balance competing interests and work together to safeguard both their national interests and the global digital ecosystem.

1.2 Research Question

The central research question of this dissertation is: How do states navigate digital sovereignty in the face of increasing global cyber threats?

This question will be explored by examining how states assert control over their digital infrastructure and data while participating in the global digital economy. It will also explore the challenges and opportunities faced by states in balancing the need for national security with the demands of international cooperation in the digital space. The analysis will focus on key issues such as data localization, international cybersecurity standards, and the role of non-state actors in shaping digital governance.

1.3 Research Objectives

1.3.1 The objectives of this research are as follows:

1.4.1 Examine the Legal Frameworks Governing Cybersecurity at the International Level: This objective will focus on understanding the existing international agreements and frameworks that regulate digital threats, cybersecurity, and data privacy. Key instruments such as the General Data Protection Regulation (GDPR), the Budapest Convention on Cybercrime, and efforts by international bodies like the United Nations will be analyzed.

1.3.2 Analyze the Tensions Between Data Localization Laws and Transnational Data Flows

Data localization laws, which require data to be stored and processed within a country's borders, have become a key aspect of many states' digital sovereignty strategies. This objective will investigate the challenges these laws present in the context of global data flows and the potential economic and diplomatic tensions that arise from conflicting regulatory regimes.

1.3.3 Assess the Roles of State and Non-State Actors in Shaping Digital Sovereignty

While states play a central role in digital sovereignty, non-state actors, including multinational corporations, technology companies, and international organizations, also influence how digital sovereignty is defined and implemented. This objective will explore the role of these actors in shaping digital policies, including the influence of companies like Google, Facebook, and Amazon, as well as the impact of international bodies such as the World Trade Organization (WTO) and the International Telecommunication Union (ITU).

1.3.4 Propose Solutions for Balancing State Sovereignty with Global Cyber Governance

Drawing on the analysis of legal frameworks, data flows, and the roles of state and non-state actors, this research will propose solutions for balancing state sovereignty with the need for global cooperation. These solutions may include recommendations for creating more robust international digital governance mechanisms, harmonizing cybersecurity laws, and improving cooperation between states and international organizations.

1.4 Conclusion

This introduction has set the stage for a detailed exploration of digital sovereignty in the context of increasing cyber threats and global connectivity. As digital technologies continue to reshape the world, the challenges surrounding digital sovereignty will remain critical to understanding the future of global digital governance. This research will seek to provide insights into how states can effectively navigate these challenges while ensuring the security and privacy of their citizens and maintaining active participation in the global digital economy. The following chapters will explore the legal, geopolitical, and economic dimensions of digital sovereignty, offering solutions for more effective governance in this evolving domain.

2 Literature review

2.1 Defining Digital Sovereignty

Digital sovereignty refers to the control a state exercises over its digital infrastructure, data, and cyberspace. This control includes regulating data flows, securing the digital environment, and asserting legal jurisdiction over the cyberspace within its borders (Yeli, 2017). The concept of sovereignty, historically associated with territorial integrity and political control over physical space, has evolved in the digital age to address the complexities of the global digital landscape. In the traditional sense, sovereignty involved a state's exclusive right to govern its land, people, and resources without external interference. However, with the rise of digital technologies and the proliferation of the internet, sovereignty now extends to the virtual realm, where states aim to protect their digital infrastructure and ensure the security of data generated within their jurisdictions (Inês, n.d.).

Digital sovereignty encompasses several critical elements: control over national data, regulation of digital services and platforms, and the establishment of cybersecurity norms to protect citizens from online threats. At its core, digital sovereignty focuses on the ability of states to maintain autonomy in an increasingly interconnected world, where global networks and digital infrastructure transcend traditional borders (Kadlecová, 2024). As such, digital sovereignty challenges the established norms of territoriality, as states now grapple with regulating and securing data that flows across jurisdictions in real-time.

The evolution from traditional territorial sovereignty to digital sovereignty has been shaped by technological advancements that blur geographic boundaries. Unlike traditional resources, data is intangible, flows seamlessly across borders, and can be exploited or compromised by actors in multiple countries (Corn & Taylor, 2017). In this context, digital sovereignty emerges as a response to the increasing need for states to maintain authority over their digital spaces. Moreover, the growing reliance on digital technologies for economic, social, and political functions has made digital sovereignty a key pillar of national security, economic stability, and public safety.

2.2 International Legal Frameworks for Cybersecurity

The rapid growth of cyberspace and the corresponding rise in cyber threats have necessitated the development of international legal frameworks aimed at governing cybersecurity and establishing norms for state behavior in the digital sphere. Several international treaties, agreements, and frameworks address cybersecurity, aiming to balance state sovereignty with the need for global cooperation in tackling cross-border cyber threats (Robles-Carrillo, 2023).

One of the earliest efforts in international cybersecurity law is the Budapest Convention on Cybercrime (2001), which was the first international treaty to address crimes committed via the internet and other computer networks. It provides a framework for cooperation between signatory states in investigating and prosecuting cybercrimes (Tsagourias, 2021). While the convention has been instrumental in creating a multilateral approach to combat cybercrime, it is limited by the absence of enforcement mechanisms and the voluntary nature of its application. Additionally, the evolving nature of cyber threats has led to calls for updating the treaty to address modern challenges such as cyber warfare and cyber espionage.

Another important development is the work of the United Nations Group of Governmental Experts (UN GGE), which has been instrumental in establishing norms for responsible state behavior in cyberspace. Through reports published in 2013, 2015, and 2021, the UN GGE has provided guidelines for state actions in cyberspace, emphasizing the need for countries to respect each other's digital sovereignty, refrain from using cyberspace for hostile purposes, and cooperate in the face of global cyber threats (Pijpers et al., 2020). The GGE's reports underscore the importance of establishing a rules-based international order for cyberspace, but the lack of binding agreements and the wide disparity in the digital capabilities of states complicate the full implementation of these norms (Schmitt & Vihul, 2017).

Regional agreements also play a key role in advancing cybersecurity laws. The EU Cybersecurity Act, adopted in 2019, is one such regional effort to strengthen cybersecurity across the European Union. It establishes a framework for the certification of ICT products, services, and processes, promoting a unified approach to cybersecurity. Additionally, the ASEAN Cybersecurity Cooperation Strategy aims to enhance cooperation among Southeast Asian countries in addressing cybersecurity threats and ensuring the resilience of digital infrastructure in the region. These regional frameworks, while effective within their jurisdictions, face challenges in addressing the global nature of cyberspace and the complexities of transnational cyber threats (Moerel & Timmers, 2021).

Despite these international and regional efforts, one of the main challenges in developing binding cybersecurity laws is the conflict between national interests and global cooperation. States often prioritize their own national security and digital sovereignty, which can lead to a lack of consensus on international legal frameworks (Chircop, 2019). The absence of a universally accepted set of cybersecurity laws means that states must navigate a patchwork of domestic and international regulations, creating a fragmented global approach to cybersecurity.

2.3 Tensions Between Data Localization and Transnational Data Flows

One of the key issues in digital sovereignty is the tension between data localization and transnational data flows. Data localization refers to the legal requirement for data generated within a state's borders to be stored or processed domestically (Heintschel von Heinegg, 2013). States impose data localization laws to protect their citizens' privacy, ensure the security of national data, and promote local economic interests. For instance, countries like Russia and China have implemented strict data localization requirements, compelling foreign tech companies to store data on local servers.

The motivations for data localization are multifaceted. From a security perspective, countries are concerned about the potential risks of data being accessed or manipulated by foreign governments or malicious actors. Data localization laws also aim to ensure that sensitive information, such as financial or health data, remains under the jurisdiction of national laws, making it easier for states to enforce their regulations (Tsagourias, 2021). Furthermore, data localization can be seen as a form of economic protectionism, as it encourages the development of local data centers and fosters growth in the domestic tech industry.

However, data localization laws often conflict with global digital trade and the seamless flow of data across borders. The global nature of the internet and the need for multinational companies to process data quickly and efficiently often require data to move across borders (Tsagourias, 2021). This creates friction between the desire to maintain control over domestic data and the reality of global data flows that underpin modern digital economies. The European Union's General Data Protection Regulation (GDPR), while emphasizing data privacy, has also sparked debates over the implications of data localization. The GDPR's requirement for strict data protection standards has led to tensions with countries like the United States, where data governance laws are less stringent. Moreover, the extraterritorial

application of the GDPR has raised concerns about the ability of states to enforce data protection laws across jurisdictions.

2.4 State vs. Non-State Actors in Digital Sovereignty

In the context of digital sovereignty, both state actors and non-state actors play significant roles in shaping the regulatory landscape. States, as the primary entities responsible for ensuring the security and stability of cyberspace within their borders, have adopted various laws and regulations to govern cybersecurity and data management. For example, many countries have enacted national cybersecurity strategies, which include measures for protecting critical infrastructure, preventing cyberattacks, and securing digital services (Gill & Ziolkowski, 2013).

The US-China tech cold war exemplifies the geopolitical conflicts that arise over digital sovereignty. The rivalry between the two countries has intensified as both seek to dominate global digital infrastructure and secure their digital spaces (Ziolkowski, 2013). The United States, for instance, has pushed for the inclusion of cybersecurity provisions in trade agreements, while China has prioritized the development of its own digital economy and imposed strict regulations on foreign tech companies operating within its borders. The competition over 5G technology, spearheaded by companies like Huawei, has become a focal point in the broader geopolitical struggle for digital control.

Non-state actors, particularly multinational technology companies, have an outsized influence on digital governance. Companies like Google, Facebook, and Amazon operate across multiple jurisdictions and are integral to the global digital ecosystem (Heintschel von Heinegg, 2013). These companies often face conflicting regulatory requirements and must navigate complex legal landscapes to ensure compliance with national laws while maintaining their global operations. Moreover, the power of these tech giants to shape global digital norms—whether through lobbying efforts or the design of platform policies—has made them key players in the discourse around digital sovereignty.

2.5 Literature Gaps

Despite the growing body of research on digital sovereignty, several gaps remain in the literature. One significant gap is the insufficient exploration of the interplay between state sovereignty and non-state actor influence. While much of the existing literature focuses on state-centric approaches to digital sovereignty, fewer studies address how multinational corporations, NGOs, and international organizations shape the regulatory landscape and influence national policies. Additionally, there is limited analysis of how cybersecurity frameworks can address geopolitical tensions and the implications of such frameworks for international cooperation. As digital sovereignty increasingly becomes a site of global competition, understanding the role of non-state actors in shaping digital governance is essential for comprehensive policy development.

Another gap is the lack of focus on the legal challenges posed by the extraterritorial application of national cybersecurity laws. While data localization and cross-border data flows have been widely studied, less attention has been paid to the difficulties faced by states in enforcing cybersecurity laws that extend beyond their borders, particularly in the context of multinational corporations and their global operations.

This chapter has outlined the key theories and frameworks surrounding digital sovereignty, reviewed existing literature on the subject, and identified gaps in current research. The following chapters will build on this foundation to explore how states navigate the challenges of digital sovereignty and the broader implications for international digital governance.

3 Methodology

3.1 Research Design

This research adopts a qualitative approach to examine state responses to digital sovereignty, focusing on doctrinal legal analysis and case studies. A doctrinal legal analysis allows for an in-depth investigation of existing legal frameworks governing digital sovereignty, providing a critical review of international treaties, national laws, and regulations. This method is particularly relevant given the complex and evolving nature of digital governance, where legal frameworks must respond to dynamic technological developments and geopolitical tensions.

The doctrinal analysis in this study will evaluate the relevant legal texts, such as international treaties (e.g., the Budapest Convention on Cybercrime) and national laws (e.g., China's Cybersecurity Law, US CLOUD Act), to identify key provisions and legal principles that underpin digital sovereignty. By examining these legal instruments, the research

will highlight the challenges and opportunities for states in asserting control over cyberspace while navigating global digital governance.

Additionally, this study utilizes case studies to contextualize the theoretical analysis. Case studies provide empirical evidence of how states balance the demands of digital sovereignty with participation in the global digital economy. The case study approach allows for a deeper understanding of the practical application of legal principles and the real-world impact of national policies on digital sovereignty. This will be particularly valuable in exploring the tensions that arise between national laws and international norms, as well as between state and non-state actors in the digital sphere.

3.2 Data Sources

The data sources for this research will include both primary and secondary materials, ensuring a comprehensive analysis of digital sovereignty.

3.2.1 Primary Sources

The primary sources will consist of international legal frameworks and national cybersecurity laws that form the foundation of digital sovereignty regulation. Key primary sources will include:

The Budapest Convention on Cybercrime (2001): This treaty provides a framework for international cooperation in combating cybercrime and addresses issues related to digital sovereignty, including jurisdictional concerns and cross-border data flows.

General Data Protection Regulation (GDPR): As a key piece of European legislation on data protection, the GDPR provides a relevant legal framework for understanding how data sovereignty intersects with privacy and cross-border data flows.

National Cybersecurity Laws: Laws such as China's Cybersecurity Law and the US CLOUD Act will be analyzed to explore how different countries regulate digital sovereignty within their borders, balancing national security with international obligations. These laws exemplify contrasting approaches to data sovereignty, with China emphasizing strict data localization and the US focusing on extraterritorial jurisdiction over digital data.

3.2.2 Secondary Sources

Secondary sources will include academic journals, books, and reports that provide theoretical and empirical insights into digital sovereignty, cybersecurity, and digital governance. These sources will offer a broader context for understanding the legal frameworks and their implications. Notable sources may include:

Academic literature on digital sovereignty, international law, and cybersecurity will help analyze the theoretical underpinnings of state control in cyberspace and the global governance challenges arising from the digital age.

Industry reports from organizations such as the World Economic Forum (WEF) and the Internet Society will provide insights into the practical challenges of global connectivity, the threats posed by cyberattacks, and the evolving trends in digital governance.

Reports from NGOs and think tanks will provide perspectives on the social and political implications of digital sovereignty, including issues related to privacy, data protection, and human rights.

3.3 Case Study Selection

To examine how different states navigate digital sovereignty, this research will analyze three key case studies, each representing a unique approach to balancing national control and participation in global digital governance.

3.3.1 European Union (EU)

The EU's General Data Protection Regulation (GDPR) serves as a landmark regulation in data protection and digital sovereignty. By examining the EU's approach to data protection and its efforts to regulate cross-border data flows, the study will assess how regional leadership in digital governance influences global standards. The EU's efforts to create a single digital market and ensure data privacy will provide insights into the challenges of managing digital sovereignty within a multinational framework.

3.3.2 China

China's Cybersecurity Law (2017) and its strict data localization requirements will be analyzed to explore how a nation-state asserts digital sovereignty through legislation that restricts foreign access to domestic data. China's emphasis on data sovereignty, coupled with its geopolitical ambitions in cyberspace, presents a distinctive model of digital governance. This case will also examine the conflict between China's regulatory approach and international norms for cross-border data flows.

3.3.3 United States

The US CLOUD Act (2018), which allows US law enforcement to access data stored overseas by US-based companies, will be explored to understand how the US balances its global leadership in the digital economy with national security interests. The US approach raises significant questions about extraterritorial jurisdiction and the conflict between national laws and the sovereignty of other states. The role of US-based tech giants, such as Google, Facebook, and Microsoft, will also be examined in this context, as these companies significantly influence global digital governance.

These case studies were selected because they represent three major players in the global digital landscape, each with a unique set of challenges and responses to digital sovereignty. By comparing these cases, the research will highlight how different states address the intersection of national security, data privacy, and international cooperation in cyberspace.

3.4 Ethical Considerations

Throughout this research, maintaining objectivity and addressing potential ethical concerns is essential. Given the geopolitical sensitivities surrounding digital sovereignty, particularly when analyzing state actors like China, the US, and the EU, it is important to approach the subject matter without bias or political agenda. The analysis will focus on legal frameworks and state behavior, avoiding political interpretations or criticisms of specific countries.

Furthermore, ethical concerns related to privacy and data protection will be carefully considered when discussing case studies involving data sovereignty and security. In particular, the research will respect the confidentiality of any proprietary data and sensitive information obtained from secondary sources. Any use of personal data or private company data in the analysis will adhere to strict ethical standards, ensuring that no confidential or privileged information is disclosed without proper consent.

The research will also consider the broader ethical implications of digital sovereignty in the global context. These include issues related to human rights, particularly the right to privacy and freedom of expression, and the impact of digital governance on marginalized communities. The analysis will take into account how the legal frameworks examined in the case studies affect individuals, societies, and global citizens, emphasizing the need for a balanced and equitable approach to digital sovereignty that respects both state interests and human rights.

3.5 Conclusion

This methodology chapter outlines the research design, data sources, case study selection, and ethical considerations for this dissertation on digital sovereignty. The qualitative approach, using doctrinal legal analysis and case studies, will provide a comprehensive understanding of how states navigate the complexities of digital sovereignty in an increasingly interconnected and cyber-threatened world. By examining key legal frameworks, national laws, and case studies, this research aims to contribute valuable insights into the future of global digital governance and the balancing act between state sovereignty and international cooperation in the digital age.

4 Data Analysis, Presentation and Interpretation

4.1 Case Study 1: The European Union's Digital Sovereignty Framework

The European Union (EU) has established a robust framework for digital sovereignty, largely encapsulated by the General Data Protection Regulation (GDPR) and its data privacy laws. The GDPR, enacted in 2018, is a comprehensive data protection regulation that has set a high standard globally for protecting personal data. By regulating how companies—both within and outside the EU—handle EU citizens' data, the GDPR advances EU digital sovereignty by asserting the region's legal authority over global tech companies. The regulation's extraterritorial reach mandates that any company dealing with EU citizens' data, regardless of its location, comply with its provisions. This expansive jurisdiction underscores the EU's ambition to control digital data flows and protect its citizens' privacy, even on the global stage.

However, enforcing the GDPR outside the EU presents significant challenges. While the regulation's territorial applicability extends to foreign companies, its enforcement in jurisdictions outside the EU depends heavily on international cooperation and the willingness of foreign governments to support EU efforts. In practice, the EU's ability to enforce compliance can be limited by conflicting local laws or lack of extraterritorial reach. For example, when non-EU countries like the US or China host tech giants that collect and process EU citizens' data, the EU faces difficulties in ensuring these companies comply with its stringent privacy rules, especially in the absence of direct legal enforcement mechanisms in these jurisdictions.

Furthermore, while the GDPR strengthens data protection within the EU, it creates a tension between privacy protection and global digital trade. The regulation imposes stringent requirements on cross-border data transfers, which can complicate the operations of multinational companies. For instance, tech companies like Google or Facebook face hurdles in ensuring compliance with the GDPR while managing global data flows. This conflict between data protection and the need for unrestricted global data flows raises concerns about potential barriers to international business and trade in the digital economy.

The EU also plays a crucial role in promoting global norms for cybersecurity and data governance. The GDPR has inspired similar laws in other regions, such as the California Consumer Privacy Act (CCPA) in the United States, as well as influencing global debates on digital sovereignty. Moreover, the EU has sought to position itself as a global leader in cybersecurity through initiatives like the EU Cybersecurity Act and its ongoing efforts to develop a common cybersecurity framework. By setting high standards for data protection and cybersecurity, the EU asserts its influence on the international stage, encouraging other regions to adopt similar frameworks to address digital governance.

4.2 Case Study 2: China's Approach to Digital Sovereignty

China presents a different model of digital sovereignty, with its Cybersecurity Law, which came into effect in 2017, and its strict data localization requirements. The law mandates that companies operating in China store data related to Chinese citizens within the country's borders. This approach is a clear manifestation of China's assertion of control over its digital infrastructure and its prioritization of national security. The country's data localization laws also aim to prevent foreign governments or companies from accessing sensitive Chinese data, thus minimizing the risk of cyberattacks or surveillance by external actors.

China's approach to digital sovereignty is grounded in the principle of cyber-sovereignty, which contrasts with the global vision of an open and interoperable internet. The Chinese model emphasizes state control over digital infrastructure and the internet, seeking to limit external influence while enhancing domestic capacity in terms of digital technologies. This system is aligned with China's broader geopolitical strategy of technological self-reliance and reduced dependency on foreign tech companies. The government's Great Firewall is one of the most prominent aspects of its internet governance, regulating and blocking foreign websites and content deemed politically sensitive or harmful to national interests.

While China's strict data localization policies have fostered greater control over its domestic digital ecosystem, they also create challenges for the country in terms of international connectivity. The restriction on cross-border data flows and the isolation of the Chinese digital market complicate China's participation in the global digital economy. However, China has positioned itself as a leader in digital governance by promoting its model of cyber-sovereignty as an alternative to Western-style internet governance. The tension between China's cyber-sovereignty model and the global open internet principles has led to increased geopolitical tensions, especially with the United States and the European Union. This friction highlights the geopolitical implications of digital sovereignty, where the control over digital infrastructures can have broader implications for international relations and global trade.

4.3 Case Study 3: United States and Global Connectivity

The United States, as a dominant player in global digital governance, seeks to balance its national interests with its leadership role in the global internet economy. The Clarifying Lawful Overseas Use of Data (CLOUD) Act, passed in 2018, exemplifies the United States' approach to balancing state sovereignty with the need for cross-border data access. The CLOUD Act allows US law enforcement agencies to compel US-based tech companies to provide data, even if it is stored overseas. This law highlights the extraterritorial reach of US jurisdiction over data, which has raised significant concerns among other countries regarding sovereignty violations and the unilateral nature of US laws. Critics argue that the CLOUD Act undermines foreign privacy protections and sovereignty by granting the US extensive powers to access data in other countries.

The US-based technology companies—such as Google, Facebook, and Amazon—are central actors in the shaping of global data governance. These companies, often operating across multiple jurisdictions, influence global data norms through their operations and lobbying efforts. The dominance of these tech giants in the global market has given the US a strategic advantage in digital governance, but it has also created tensions with other countries that are concerned about data privacy and national security. The US faces the challenge of balancing its role as a global leader in internet governance with its national security interests, particularly when it comes to the protection of personal data and privacy.

The conflict between national security interests and the global influence of US technology companies is one of the central tensions in US digital sovereignty. On one hand, the US aims to maintain leadership in global connectivity by promoting free and open internet principles. On the other hand, it must navigate the complexities of international cooperation in the face of security threats such as cyberattacks and surveillance. The extraterritorial nature of US data laws and the influence of US tech companies complicate this balance, creating friction with countries that advocate for stricter national control over digital infrastructures.

4.4 Common Themes and Tensions

Across the three case studies, several common themes and tensions emerge regarding digital sovereignty:

Data Localization vs. Global Connectivity: Each case highlights the tension between data localization laws (such as those in China and the EU) and the need for unhindered cross-border data flows. While data localization is seen as a way to protect national security and privacy, it can also stifle international trade, create barriers to innovation, and disrupt global business operations.

The Role of Non-State Actors: Technology companies are powerful non-state actors that significantly influence global data governance. These companies, especially those based in the US, shape the norms and practices around digital sovereignty, often in opposition to national regulatory efforts. Their role in influencing sovereignty raises questions about the balance of power between states and corporations in the digital realm.

Geopolitical Rivalries: Digital sovereignty is increasingly viewed through a geopolitical lens, particularly in the rivalry between the US and China. As both countries assert their models of digital governance, their competing visions of sovereignty have profound implications for the future of global digital governance.

4.5 Proposals for Balancing Digital Sovereignty and Global Governance

To address the tensions between digital sovereignty and global governance, several proposals can be made:

Strengthening Multilateral Frameworks for Cybersecurity: International frameworks like the Budapest Convention and UN initiatives should be strengthened to create binding agreements on cybersecurity. This would help avoid fragmentation in global digital governance and encourage collaboration on cross-border cybersecurity issues.

Developing Global Data Governance Standards: The creation of global standards for data governance that respect national sovereignty while enabling cross-border data flows is critical. Such standards could help reconcile the tension between data protection and digital trade, providing a roadmap for international cooperation on data governance.

Promoting Public-Private Partnerships: Governments should collaborate with tech companies to address cybersecurity threats and ensure the safe flow of data across borders. Public-private partnerships can help mitigate the influence of non-state actors while promoting cyber resilience and data protection.

By addressing these challenges and fostering international cooperation, it is possible to strike a balance between digital sovereignty and the need for global connectivity, ensuring that the benefits of a globally interconnected digital world are realized without compromising security, privacy, and national sovereignty.

5 Conclusion

This dissertation has explored the concept of digital sovereignty and the challenges it poses in the context of global cyber governance. Through an analysis of case studies from the European Union, China, and the United States, key insights have emerged regarding the ways states navigate the tension between asserting control over their digital infrastructures and participating in an interconnected global digital ecosystem. The European Union's emphasis on data

protection, as demonstrated by the GDPR, underscores its desire for digital sovereignty through stringent regulation of global tech companies. Conversely, China's Cybersecurity Law and data localization policies reflect a more insular approach to digital governance, prioritizing national security concerns. The United States, meanwhile, exemplifies the challenge of balancing its leadership in global digital infrastructure with national security interests through laws like the CLOUD Act and the extraterritorial reach of its technology companies.

These case studies highlight both common strategies and significant conflicts. While all three regions seek to protect their sovereignty, they face competing priorities: the need to control domestic digital infrastructure and data flows, while still engaging with the global market and fostering innovation. The tensions between data localization laws and transnational data flows have emerged as a central theme, exacerbated by geopolitical rivalries and the increasing influence of non-state actors like tech companies. These dynamics illustrate the complexities of reconciling digital sovereignty with the need for international collaboration in cyber governance.

5.1 Contribution to Knowledge

This dissertation contributes to the growing body of knowledge on digital sovereignty by offering a comprehensive analysis of how states are navigating the complexities of cyber governance in a fragmented global landscape. It expands on existing literature by exploring the interactions between state and non-state actors and how these influence digital sovereignty. It also provides insight into how international frameworks like the Budapest Convention and GDPR have shaped and challenged the sovereignty of states in cyberspace. Through the case studies, the research highlights the conflicting priorities of national security, economic interests, and global digital cooperation, illustrating the challenges faced by states in achieving both sovereignty and cooperation in a rapidly evolving digital world.

Furthermore, this dissertation explores the evolving role of non-state actors, particularly large tech companies, and their influence in shaping global data governance norms. It underscores the need for a more unified approach to digital sovereignty, where states and non-state actors can cooperate effectively to ensure both national security and global connectivity.

5.2 Recommendations

5.2.1 Strengthening International Cybersecurity Frameworks:

In light of the challenges faced by states in maintaining sovereignty while participating in global cyber governance, the expansion and enforcement of multilateral cybersecurity agreements are critical. The Budapest Convention on Cybercrime, as one of the few binding's international treaties on cybersecurity, should be broadened and modernized to include newer digital threats such as AI-driven cyberattacks and IoT vulnerabilities. Strengthening multilateral frameworks would promote cooperation and reduce the risk of fragmentation in the global cyber landscape. Additionally, fostering cross-border cybersecurity collaboration among states is essential to address increasingly sophisticated cyber threats that transcend national borders.

5.2.2 Harmonizing Data Governance:

Given the tension between data localization and cross-border data flows, there is an urgent need to develop global guidelines that balance these two conflicting priorities. Such guidelines should aim to protect privacy and national security while facilitating the global exchange of data necessary for business and innovation. The EU's GDPR offers a strong model in terms of protecting data, but global standards should also address the economic needs of countries that depend on data flows for digital trade. A unified international framework could help align policies across regions, mitigating the risks of data protectionism and creating a balanced approach to global digital governance.

5.2.3 State-Non-State Collaboration:

To ensure secure and sovereign cyberspace governance, enhanced cooperation between states and technology companies is essential. The influence of tech giants in shaping data governance cannot be overlooked, and their role in cybersecurity and data protection must be integrated into national and international regulatory frameworks. Governments should engage with non-state actors through public-private partnerships to create more robust cybersecurity infrastructures and ensure the protection of critical data. Tech companies should be held accountable for their role in shaping the digital landscape, particularly in terms of data privacy, security, and global digital trade.

5.2.4 Address Geopolitical Rivalries:

Geopolitical tensions between major powers, such as the United States and China, threaten to divide the global digital space. These rivalries highlight the need for inclusive international forums, such as the UN GGE (Group of Governmental Experts), to create shared cyber norms that can mitigate conflicts. Such forums should encourage dialogue and cooperation on issues of cybersecurity, data governance, and digital sovereignty, promoting norms that respect both national interests and the necessity of a globally interconnected digital ecosystem. The creation of mutually agreed-upon rules could help alleviate the risks of fragmented digital governance and prevent a digital arms race that further deepens geopolitical divides.

5.3 Future Research Directions

Future research could explore the impact of emerging technologies on digital sovereignty, particularly the role of artificial intelligence (AI) and the Internet of Things (IoT). These technologies present new challenges to both cybersecurity and data governance, as they involve the collection and analysis of vast amounts of data from a variety of sources. Research could focus on how these technologies are reshaping the power dynamics of digital sovereignty, with an emphasis on ethical implications, privacy concerns, and the need for robust regulation.

Moreover, future studies could investigate regional approaches to digital sovereignty in developing economies, particularly in regions such as Africa and South America. These regions face unique challenges in balancing digital sovereignty with the need for technological development and global digital trade. Research in these areas could shed light on how developing economies are navigating digital sovereignty and contribute to the global discourse on cyber governance.

5.4 Final Reflections

In conclusion, digital sovereignty is a critical issue for safeguarding national interests in the face of transnational cyber threats. As states continue to confront challenges related to cybersecurity, data protection, and geopolitical rivalries, the need for a balanced approach to digital sovereignty is more urgent than ever. This research has shown that while states must assert control over their digital infrastructures, achieving effective governance requires global cooperation to address the transnational nature of cyber threats. The future of digital sovereignty lies in multilateral frameworks, collaboration between states and non-state actors, and the development of shared cyber norms that respect both national sovereignty and global interconnectedness. Only through this approach can we ensure a secure and sovereign cyberspace that fosters innovation, privacy, and cooperation in an increasingly connected world.

Compliance with ethical standards

Statement of ethical approval

Ethical approval was obtained.

Statement of informed consent

Informed consent was obtained from all individual participants included in the study.

References

[1] Chircop, L. (2019). Territorial sovereignty in cyberspace after'Tallinn Manual 2.0'. Melbourne Journal of International Law, 20(2), 349-377.

[2] Corn, G. P., & Taylor, R. (2017). Sovereignty in the Age of Cyber.

[3] Fauzi, E., Citra, H., Marwenny, E., & Alfitrianti, N. (2024). Control of Personal Data and Cyber Space by Global Digital Platforms in Relation to Indonesia's Digital Sovereignty. Jurnal Ilmiah Ekotrans & Erudisi, 4(1), 149-157.

[4] Gill, T. D., & Ziolkowski, K. (2013). Non-intervention in the Cyber Context. Peacetime Regime for State Activities in Cyberspace International Law. International Relations and Diplomacy. NATO CCDCOE, Tallinn, 217-238.

[5] Gur, B. A. (2022). Cybersecurity, European digital sovereignty and the 5G rollout crisis. Computer Law & Security Review, 46, 105736.

[6] Heintschel von Heinegg, W. (2013). Territorial sovereignty and neutrality in cyberspace. International Law Studies, 89(1), 17.

[7] Inês, R. I. T. O. China's Cyber Sovereignty And The United Nations: Navigating Tensions In Global Cyber Governance.

[8] Kadlecová, L. (2024). Cyber Sovereignty: The Future of Governance in Cyberspace. Stanford University Press.

[9] Mathur, S. Digital Sovereignty: Balancing Security, Identity And Global Hegemony. NAVIGATION THE DIGITAL FRONTIERS: NEW PARADIGMS OF TECHNOLOGY AND SOCIETY, 19.

[10] Moerel, L., & Timmers, P. (2021). Reflections on digital sovereignty. EU cyber direct, research in focus series.

[11] Mueller, M. L. (2020). Against sovereignty in cyberspace. International studies review, 22(4), 779-801.

[12] Perritt Jr, H. H. (1997). The Internet as a threat to sovereignty-thoughts on the internet's role in strengthening national and global governance. Ind. J. Global Legal Stud., 5, 423.

[13] Pijpers, P. B., & van den Bosch, B. (2020). The 'Virtual Eichmann': on Sovereignty in Cyberspace. Amsterdam Law School Research Paper, (2020-65).

[14] Pohle, J., & Thiel, T. (2020). Digital sovereignty. Pohle, J. & Thiel.

[15] Robles-Carrillo, M. (2023). Sovereignty vs. digital sovereignty. Journal of Digital Technologies and Law, 1(3), 673-690.

[16] Schmitt, M. N., & Vihul, L. (2017). Sovereignty in cyberspace: lex lata vel non?.

[17] Tsagourias, N. (2021). The legal status of cyberspace: sovereignty redux?. In Research Handbook on International Law and Cyberspace (pp. 9-31). Edward Elgar Publishing.

[18] Tsagourias, N. (2021). The legal status of cyberspace: sovereignty redux?. In Research Handbook on International Law and Cyberspace (pp. 9-31). Edward Elgar Publishing.

[19] Wu, C. H. (2021). Sovereignty Fever: The Territorial Turn of Global Cyber Order. Zeitschrift für ausländisches öffentliches Recht und Völkerrecht/Heidelberg Journal of International Law, 81(3), 651-676.

[20] Yeli, H. (2017). A three-perspective theory of cyber sovereignty. Prism, 7(2), 108-115.

[21] Ziolkowski, K. (2013). General principles of international law as applicable in cyberspace. In Peacetime regime for state activities in cyberspace (pp. 135-188). Tallinn: NATO CCD COE Publications.