SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 4264-4272
Open Access. Online & Print

DOI: 10.5281/zenodo.12426475

DIGITAL SOVEREIGNTY STRATEGIES AND THEIR ROLE AS A TOOL FOR INTERNATIONAL COMPETITION: ANALYTICAL STUDY

Dr. Hayder Abed Kadhim[1], Shefaa Khaleel[2]

[1 2] College of Political Science University of Baghdad

Received: 12/09/2025
Accepted: 23/02/2026

Corresponding author: Dr. Hayder Abed Kadhim (haidar.abid@copolicy.uobaghdad.edu.iq)

ABSTRACT

Our research will extend the examination of the digital sovereignty as the means of competing in the international relations or fulfilling the national interest in the context that the contemporary international system has established. Instead of talking about it as a technical issue per se, we demonstrate how the digital world has evolved into a different technical space of administration into a critical battlefield where power, influence and international order are also re-traded. Thus, such significant aspects of digital sovereignty as data control, technical standards and infrastructure are also considered in our analysis. The method predominantly used in the research is concept analysis. It deconstructs Digital Sovereignty as concept by both: the theoretical and practice lens to expose differences among powers in terms of how it is applied by looking at examples that it draws based on the experience of US, European Union Russia and China. It is possible, through this, to get a better understanding of how this process affects on power equilibriums or international competition. The main finding of the conclusion of the study is that digital sovereignty is a multi-layered instrument that balances national security; and oversees regulatory regulations, at the same time, it increases the strategic and digital influence of a state on an international level. Moreover, our study sheds light on the idea that the use of digital sovereignty by competing powers is usually very diversified in relation to the possibility of success in an international competition. Viewed through the prism of the global-stage perspective, this study believes that, in any likelihood, can generate more holistic analysis models that would combine political, economic and technological aspects of digital era. It also notes that the digital sphere control has turned into a significant consideration in estimating power and prestige in the 21st century.

KEYWORDS: Digital sovereignty, International competition, Digital space, and Digital strategy.

1. INTRODUCTION

State sovereignty is a concept that used to be rigidly implemented over the physical boundaries and the Westphalian tradition of 1648, but is now being redefined by the very sheer mass of the digital age (Al-Madani, 2021). In this respect, power is no longer considered as land, sea, air, or even space. Instead, it has infiltrated into a constantly growing dimension in which data, AI and information infrastructure determines the new forms of what international security can actually be. This new state-of-affairs does not, by having said the above, indicate that it is a passive evolution. The dominant actors in the international scene like the United States, China, Russia, and the European Union are weaponizing the digital strategies to defend their national identities and simultaneously impose their strategic will on other nations. These countries, as Shocker (2022) notes, resort to digital control as a means of self-protection at home and attempt to gain an edge over other countries. According to the U.S. approach of conditional openness, which favors its tech giants globally, to a next century of China with its strict Great Firewall and Digital Silk Road programs, these forces are indeed competing to establish the regulatory and technical standards that will officiate the next century (Fratini et al., 2024).

Ultimately, the ability to control the flow of bits and bytes, certainly along with the physical subsea cables that carry them, has become a an undeniable measure of a nation's prestige and its capacity to see through the volatile nature of international competition.

2. THE CONCEPT OF DIGITAL SOVEREIGNTY

The concept of digital sovereignty, and the meanings it covers, requires breaking down the concept and delving into its content to understand its essence. This is needed to reach a deeper understanding of digital sovereignty by clarifying its paths in light of the developments on the international stage, and the interactions of countries and global actors within the international system. This is especially important since the concept of sovereignty is one of the most prominent ideas linked to the security and independence of states, making it one of the concepts that has occupied the minds of thinkers and researchers throughout history. The concept of sovereignty has evolved over the past centuries, becoming closely associated with the idea of the nation-state, emerging clearly in the late sixteenth and seventeenth centuries in European countries, coinciding with the rise of the state as a legal entity, particularly after the Treaty of Westphalia in 1648, which established the fundamental political principles in Europe, most noticeably the principle of stat-e sovereignty (Al-Madani, 2021, p. 36; Fahmi, 2022, p. 38).

By the end of the Cold War, with the collapse of the Soviet Union in 1990, and the spread of liberal thought represented by democracy and free-market economics (Khalaf, 2024, p. 25), instead of the concept of sovereignty, the concept of national sovereignty emerged. This singles out the sovereign capacity of a nation to rule within its recognized borders and interact with others as set out by treaty. In this way, national sovereignty is considered a foundation for protecting the state and its independence, and it also entails respecting its relations with other countries under international law. Thus, the concept of sovereignty shifted from an absolute notion to a flexible one in line with international laws. This flexibility in sovereignty became evident in relations between states and was reflected in international relations. States moved from isolation to cooperation and the alignment of interests, and any action a state takes without international legitimacy could jeopardize its national sovereignty (Al-Dulaimi, 2025, pp. 264–266), especially given the changes in the international system, which redefined global dynamics and altered the balance of international power (Ali, 2025, p. 4).

Amid the scientific, technological, and strategic developments in the late 20th century and the early 21st century, the concept of national sovereignty changed. Traditional wars no longer cause reductions in a country's internal sovereignty. Instead, countries started using new forms of modern warfare, such as 'hybrid wars,' which rely on various advanced scientific and technological techniques. This has led to sovereignty being penetrated through different tools of technological, technical, and digital warfare, including things like online propaganda, cyber programs, artificial intelligence applications, smart missiles, drones, and more (Al-Ali & Hamid, 2022, p. 175). In light of the above, state sovereignty in the digital age is no longer what it used to be. With the arrival of the twenty-first century, along with its scientific, technological, and digital developments, and the comprehensive reliance of countries on electronic technologies and digital tech—which has become the fifth dimension of a country's power after land, sea, air, and space—the concept of traditional sovereignty has declined. Countries have become more interconnected, which has led them to restrict their citizens and set new digital boundaries,

allowing them to regain control over their sovereignty. This gave rise to what is known as the concept of Digital Sovereignty.

Advanced information technologies have certainly imposed a new situation on countries in the international community, both developed and developing. The state has become threatened through its sovereign space, which has prompted it to adopt policies that enhance its digital sovereignty amid ongoing rapid technological developments. Digital sovereignty only emerged as a result of the internet and technological advancements surpassing the traditional boundaries of state sovereignty (Saadi, 2020, pp. 300–320). Moreover, global rivalries are day by day playing out through technology and as such they are pushing governments to fight for digital autonomy and put more money into protecting their online interests (Lambach & Oppermann, 2022, pp. 699–700)

Returning to the concept of digital sovereignty and its origins, the concept emerged in 2001, especially after the events of September 11 and alongside the U.S. Patriot Act, and was called data sovereignty at the time. Since the internet was limited to a small number of users back then, sovereignty was restricted to expert circles concerning the digital civil society in the United States, as it was the main dominant force over networks, communication technologies, digital platforms and services, cloud computing, and digital infrastructure. Because it showed such advanced, one-of-a-kind technology, it was capable of generating and archiving data on a worldwide scale (Lambach & Oppermann, 2022, pp. 699–701). It had near-total control over internet networks and communication technologies, which allowed it to access data anywhere and under any circumstance. This actually led to many developed countries to seek achieving digital sovereignty, not just over their physical territory but also over their digital one too and the push here is to break free from the reliance on U.S. platforms and everything tied to them in the digital sphere. (Thumfart, 2022, pp. 6–12)

In the early 2000s, governments started introducing the concept of digital sovereignty, aiming for complete state control over regional, spatial, and digital domains. This came as countries began to see digital transformation primarily as a geopolitical threat, even before considering it a threat to their sovereign or digital security. As a result, countries started developing strategies to solidify their digital sovereignty within their territories, as well as setting regulatory standards to monitor and control the flow of data and information coming in and out. However, these strategies inevitably clash with global digital interconnectivity. Not only that, but countries also began creating their own standards, software, and different digital systems to break away from American digital dominance (United Nations, 2021).

Consistently with what has been mentioned, the concept of digital sovereignty refers to a state's ability to control its digital destiny, the flow of data, and manage the entire supply chain of AI software and applications, starting from data control to controlling devices and software (Martynova & Shcherbovich, 2024). Although the concept of digital sovereignty started being mentioned in 2001 and entered scientific and research discussions, it was not addressed as a political concept by developed countries until 2010, after the European Union sought to include it in its digital infrastructure. Focus on it increased even more after the Snowden leaks in 2013 and thanks to this, governments started to push for a say in how things go digital and give their local businesses the urge they need to compete (Glasze et al., 2023, pp. 930–938)

In light of this, Chinese President Xi Jinping defined digital sovereignty as the right of every nation-state to choose its own path in cyber development and its own model for regulation and internet policies, without interference from other countries Digital sovereignty is also defined as the state's ability to determine its destiny in the digital world, as well as the ability of individuals and economic institutions to use digital technologies autonomously in order to delineate and do their roles independently and securely in the digital age (Pohle, 2020, p. 8).

Another definition is offered by García (2024, p. 2) who described it as legitimate digital control over the digital world and this essentially is about a country having the final say over its digital landscape, from how data is handled to imposing a ban on specific actions by international tech companies.

Accordingly, countries' efforts to strengthen their digital sovereignty in their geographic location and digital space stem from the threats and risks posed by other countries and actors, who have what it takes to interfere with digital services and government communication technologies (Jansen et al., 2023, pp. 2–3). Especially since digital sovereignty controls data, software like artificial intelligence, standards and protocols like 5G networks, domain names, and more (Chander & Sun, 2023, p. 6).

From the above, it can be said that the spread of

the internet and technological advancements has led to the creation of new challenges for countries and brought about different kinds of threats, not just at the security and military levels, but extending to other areas as well. In this context, the concept of digital sovereignty emerged as a means to manage these challenges, reduce threats, or overcome them. According to the researcher's perspective, digital sovereignty is a comprehensive framework encompassing all of a state's digital capabilities and resources, enabling it to operate independently and safely in the digital world. In other words, it is self-designed and does not rely on other countries' technologies to safeguard its national digital security.

3. THE CONCEPT OF INTERNATIONAL COMPETITION

With the development of the international system and the changing balance of power within it, the methods and tools of international competition have evolved. These methods are no longer limited to traditional wars and the use of military force to achieve objectives. Instead, more advanced and influential tools now exist that impact overall relations between countries, including technological competition, economic wars, digital competition, as well as media and cultural influence, which often contribute to intensifying competition. International competition represents a state of rivalry between countries to achieve their national interests, whether economic, political, military, technological, digital, or other interests. This competition is often conducted peacefully, though it can sometimes escalate into conflicts reaching the level of war.

The concept of international competition has shifted from the field of international economic relations to the realm of international relations at all levels, especially with the increasing interdependence between countries in various areas. It is defined as a state of interaction that occurs between two or more international parties, characterized by a peaceful nature, away from any form of violence, tension, or conflict, in a way that does not negatively affect the nature of relationships between its parties (Al-Damdardash, 2020, p. 61). It is also defined as a situation or state that brings together two or more international parties who decide to engage in competition based on rational calculations, focusing their efforts and resources on achieving benefits and interests provided by a certain environment in the international system, without resorting to the use of military force or violence to obtain these benefits and achieve these goals. (Nadhir, 2014).

Since international relations are continuous and ever-changing, competition between countries can be positive and turn into cooperation, especially in situations where cooperation is the best way to achieve common goals, such as reducing potential risks and facing various threats. On the other hand, competition can take a negative turn and evolve into conflict.

Based on this, international competition is defined as the imbalances present in the international community, which can grow and take the form of conflict if not addressed, especially since countries often seek to maximize their gains according to the concept of national interest, in a way that contradicts the interests of other countries. This leads to a state of competition, which may be limited to specific areas such as economic competition, or may include several areas like military and civilizational competition. International competition is also defined as a situation where two or more parties disagree over incompatible goals, whether those goals are real or perceived, or over limited resources (Bouzidi, 2021, pp. 322–323).

Accordingly, the change in the elements of power and competition among rival international powers reflects a comprehensive nature, aiming to achieve greater gains and to expand the scope of dominance and influence (Dawood & Jasem, 2023, pp. 170–171).

Consistent with this, international competition in the digital age has become something absolutely indispensable, as countries cannot stop it amid rapid digital developments, especially with scientific breakthroughs in technical and digital fields. This is necessary to keep up with ongoing scientific and digital developments on the international stage, not only to achieve their national interests but also to gain a distinguished position in the international community. Hence, the researcher defines international competition in the digital age as the effort of states and other actors in the international system to achieve their highest strategic goals, their overall interests, and their scientific and technological advancement, in order to obtain a prominent international position and to avoid various types of risks and threats, particularly digital ones, which require keeping up with digital technological developments.

In this way, international competition appears across various fields as key factors representing the global landscape on the international stage.

4. DIGITAL SOVEREIGNTY STRATEGIES AFTER 2001.

4.1. Digital sovereignty strategies from an international relations perspective

Digital sovereignty strategies from an international relations perspective relied on several key axes, aimed at achieving digital independence for countries. Although these strategies vary depending on a country's political system, its technical capabilities and resources, and its geopolitical goals, they converge on several main globally recognized axes, which are as follows:

• Data Localization Strategy: Data represents a critical importance for countries' cybersecurity, as the vast potential of data serves as an empowerment factor for countries and a means to enhance their capabilities. The growing reliance on data has led to the emergence of new challenges, including data security and privacy breaches resulting from the data collection and usage process.Third: Digital Sovereignty Strategies After 2001.

4.2. Digital sovereignty strategies from an international relations perspective.

Digital sovereignty strategies from an international relations perspective relied on several key axes, aimed at achieving digital independence for countries. Although these strategies vary depending on a country's political system, its technical capabilities and resources, and its geopolitical goals, they converge on several main globally recognized axes, which are as follows:

• Data Localization Strategy: Data holds great importance for countries' cybersecurity, as the vast potential of data serves as an enabling factor for nations and enhances their capabilities when used effectively. The increasing reliance on data has led to new challenges, including data security and privacy breaches resulting from the process of collecting and using data (Chander & Sun, 2023, pp. 264–265). This has prompted countries to respond to these challenges and work on protecting personal data from cyber threats and unauthorized access. Strategies to address this have taken two paths: the internal safeguards path, which involves measures and procedures applied within the country and its institutions to ensure control over incoming data, and the external safeguards path, which involves reforming data protection laws worldwide, for example, the GDPR law issued by the European Union in 2016.(Wu, 2021, pp. 5–6)

So, the concept of data localization refers to all the procedures, policies, and programs used to manage data, whether it is data related to individuals—be it personal, financial, commercial, or other—or data related to government institutions, which must be stored within the country's territorial boundaries (Abd al-Azim et al., 2023, pp. 106–107).

• Data Sovereignty Strategy: In the context of a globally connected digital landscape, the concept of data sovereignty has emerged as a key concern for countries, tech companies, institutions, and even individuals. With the flow of data on international networks, nations and other actors of the international system have ensured that they have sovereignty over their data. This is particularly so following the fast-paced change in technology and diffusion of cloud computing that has transformed the manner in which data is created, processed, and stored. Although these developments have created unprecedented opportunities in the digital field, they have also brought significant complexities related to data governance, privacy, and legal compliance with underlying laws (Digital Samba, 2025). The data sovereignty strategy refers to imposing control over the flow of data entering a country through regulatory measures and local laws to manage how data is collected, stored, and processed. This strategy works hand in hand with the data localization strategy and is closely tied to it (Araya et al., 2023, p. 18)

• National Digital Infrastructure and Self-Reliance Strategy: This strategy focuses on countries developing independent internet networks, creating national operating systems, or alternatives to foreign apps like WeChat in China instead of WhatsApp, and setting up national data centers instead of relying on foreign servers. This strategy promotes self-reliance and encourages countries to digitally depend on themselves (Shoker, 2022, p. 7).

• National Technological Capacity Enhancement Strategy: This refers to supporting national technology companies to become competitive with major foreign companies, such as China's support for its national technology companies like Huawei and Alibaba; as a step to ensure its digital sovereignty, protect its data from flowing across its sovereign borders, as well as safeguard its internal infrastructure from incoming data flows. This strategy also requires investment in artificial intelligence, cloud computing, and emerging technologies (such as autonomous robots capable of making decisions, and generative artificial intelligence (Lilkov, 2023, pp. 177–178).

• Cybersecurity Legislation Strategy: This involves establishing laws to protect critical digital infrastructure from cyberattacks and security breaches, as well as adopting sanctions against attacks or foreign encroachments in the digital space (Ishkhanyan, 2025, p. 6)

• Digital sovereignty strategy according to Nash equilibrium: This strategy is considered a hybrid

approach to digital sovereignty, meaning it is both cooperative and non-cooperative, used when self-reliance is not feasible. This strategy applies the concept of equilibrium from game theory to the digital and cyber domain, where countries or actors aim to achieve digital independence and stability in digital sovereign decisions without having any incentive to change their strategy, as long as the strategies of other parties remain fixed. In this strategy, the Nash equilibrium is represented by the fact that no player or international actor can improve their position by changing their strategy alone, as long as the other parties do not change theirs (Shoker, 2022, pp. 8–9). It is worth noting here that Nash equilibrium was named after its discoverer, American mathematician John Nash (1950), and represents one of the most important concepts in game theory. It achieves the optimal outcome for the game by taking into account the moves and actions of opponents(Chen, 2025). See Table (1) below.

Table 1: The digital sovereignty strategy in light of the Nash equilibrium.

Element	Description
Technological autonomy	Reducing dependence on external technology providers, particularly geopolitical rivals.
Cyber power balance	Ensuring that no individual action leads to escalation or a reaction that harms the national interest.
Cyber deterrence	Developing digital capabilities that dissuade other parties from attacking the digital environment.
Partner diversification	Avoiding reliance on a single technology partner, thereby reducing risks and threats.
Data restriction	Enacting laws and regulations that restrict the transfer of data across national borders.

Source: Adapted by the researcher from Shoker (2022, pp. 8–9); Chen (2025).

In line with the above, digital sovereignty strategies have become a tool of geostrategic power in the digital age. They go beyond data protection to become a central strategy in international relations, especially since the concept of digital sovereignty could potentially redraw the balance of power and authority between countries, representing fertile ground for competition among states over digital technological influence, economic influence, and security influence.

4.3. Digital sovereignty strategies from the perspective of major and superpowers

In the context of the modern world of global competition, Boost (2025) defines digital sovereignty as one of the main pillars of the superpowers who declare that national security now no longer depends only on the authority of the countries of their cyberspace and the safety of the flows of data and biotechnological resources. In this context, the US establishes itself as the dominant force in terms of technology globally adhering to the policy of conditional openness combined with a strategy of technological dominance.

Instead of an unchanging status, this position can be characterized by Meneses (2025) as a calculated attempt to be first in the transformative areas, such as semiconductors and artificial intelligence and at the same time develop global cybersecurity standards that align with American interests. The US here sees its alliances to embolden its allies and lock out its competitors such as Russia and China in the very infrastructure that in fact makes power in the 21st century.

Among the main pillars of the United States' digital sovereignty strategy, the following points are highlighted:

- Supporting American technology companies that transcend national borders (Roudani, 2025), such as Google, Microsoft, Amazon: because they have come to represent one of the most prominent international actors influencing the global balance of power (Manati & Alwan, 2024, p. 1815). In the digital age, power is represented by information and data flows, algorithmic influence, and the development of cyberspace, which is what the major American giant companies possess, and they enjoy the support of the United States for increasing its global dominance in the digital field.(Roudani, 2025).
- Controlling internet infrastructure like the DNS system: This is the Domain Name System, which converts website names into numerical addresses that computers understand. It consists of several servers and undersea cables, which carry 95% of the world's internet data and control how users access the internet. In this context, the United States dominates many servers, being the largest power in funding and building the huge undersea cables that connect the continents. This gives it wide influence in managing these servers and domains worldwide, which has pushed major powers to try to create their own domains and servers, aiming to protect their digital infrastructure and reduce American dominance in this field.
- After 2001, the United States, as the sole superpower in the international system and responsible for promoting stability and protecting international security and peace (Kadhim & Abd, 2020, pp. 14–15), strategically used its digital sovereignty to boost its digital superiority and maintain its position in the international digital competition. It did this through several dimensions

that turned technology, digitalization, and data into a new and central weapon in international relations. Notably, it follows a different approach, prioritizing national security and law enforcement access to data over limiting foreign influence (Fratini et al., 2024, pp. 14–20). It is worth pointing out that American police and federal agencies have huge leeway to demand data, prospect that makes other world leaders sweat over how much information the U.S. actually controls (Blinken, 2021–2025, pp. 6–12)

B) China: Centralized Control and Self-Development.

With the acceleration of global digital transformation, China has emerged as one of the key international players aiming to shape the global digital system in a way that aligns with its top interests, national security, and political foundations. Here, we see China doubling down on "cyber sovereignty," using it as a blueprint to keep a tight domestic control while projecting its digital influence globally.

This strategy was based on the following:

- China's digital sovereignty strategy is based on building a comprehensive and closed digital system that is subject to state control and managed according to strict laws that regulate digital content, data, and digital infrastructure. China also works on developing national alternatives to Western technology in the fields of artificial intelligence, cloud computing, operating systems, communication networks, and artificial intelligence, ensuring reduced dependence on foreign sources and increasing technological independence. China has developed its legislative approach in a way that heavily relies on directives from the central government. The implementation of China's national strategy in 2017 was a decisive step in moving from a flexible governance system to a stricter system, especially regarding supervision over data, algorithms, and digital technology. In 2021, China enacted the Personal Information Protection Law (PIPL), representing the national General Data Protection Regulation, which requires technology companies operating in China to classify their data and store it locally within the country. This matter is considered a crucial element in establishing digital sovereignty of China.(Larsen, 2022)
- China also launched the regulations for managing algorithmic recommendations for internet information services, which came into effect in 2022, regarding the regulation of artificial intelligence. These are considered the first regulations of their kind in the world. With this, China has increased the value of its leading tech companies, such as Baidu, Alibaba, and Huawei, strengthened the value of Its economy, and contributed to protecting its digital and national security.(ibid)
- China aims to export its digital model through digital initiatives like the Digital Silk Road, which is seen as a digital extension of the Belt and Road Initiative. China provides digital infrastructure, such as 5G networks, smart cities, and submarine cables, to developing countries, based on a regulatory model that aligns with state sovereignty.(Skoker, as cited in original, pp. 179–180)
- Expanding the Great Firewall, which is considered the most comprehensive system for internet censorship and surveillance. It monitors digital content and includes a wide range of legislative measures and technological controls designed to regulate the internet nationally by blocking access to foreign websites and filtering digital content based on keywords that are seen as a threat to Chinese digital and national security. It blocks outside money from finding it way into China's tech sector while simultaneously pushing for the use of homegrown digital tools instead (Youvan, 2024, pp. 2–3)
- In 2025, China launched its national security strategy, which set comprehensive standards for protecting its national security. Regarding the scientific, digital, and technological aspects, China focused on speeding up self-reliance and making strong efforts in key technologies such as acquiring raw materials, advanced chips, and industrial software China aims to achieve a number of goals through the aforementioned strategy, which include the following:

1. Achieving technological independence to reduce reliance on Western technologies.
2. Possessing offensive capabilities in cyberspace.
3. Implementing advanced information warfare strategies through cooperation between the state and its leading companies, such as Huawei.

In line with the above, China's digital sovereignty strategy represents a significant shift in global power dynamics. China is not just seeking to protect its national security and domestic society from external influences, but also aims to reshape the global digital system.

Based on the above, and with the start of the second millennium, the world moved from a traditional digital model to a modern digital model, described as digital sovereignty, as a central element in international politics and the digital economy, based on highly intelligent digital technologies. The

rapid developments in internet technologies, cloud computing, artificial intelligence, and technological supply chains have led to a new positioning of countries, pushing them to adopt multiple options in managing their digital interests. The major powers adopted conflicting strategies: the United States took a more liberal digital approach, while China adopted a strict control model. There also emerged an intermediate strategy based on Nash balance, representing a balance point between trying to achieve self-reliance and engaging in international cooperation.

5. CONCLUSION AND FINDINGS

This study has shown that digital sovereignty is not a purely technical matter but a framework with multiple dimensions through which states can pursue security, influence, and prestige in the international system.

Although the United States, China, Russia and European Union use their own unique strategies of conditional openness to strict control the overall goal, however, stays the same and that is to protect national interests and establish digital era strategic power.

The results indicate that:

1) The role of digital sovereignty as a factor stabilizing the national security and as a process of forming regulatory spaces is played simultaneously. Its application is not, however, even.
2) Differences in the political system, technological potential, and geopolitics priorities imply that there is a variety of strategies, and this actually generates imbalanced impacts on the balance of power.
3) Notably, the study emphasizes that the concept of digital sovereignty is not defensive, but it also possesses a competitive advantage since the ability to control data, infrastructure, and standards is becoming an ever more determining factor in the establishment of states in world hierarchies.
4) Coexisting with this is the fact that the quest toward digital autonomy is frequently brought into conflict with the facts of interdependence that consequently raises the question as to whether full sovereignty in the digital realm is indeed possible.
5) Digital sovereignty is to be perceived and thereby operated as a national requirement and a disputed field of international struggle.
6) Future studies should look into the evolution of new technology including generative AI, quantum computing, and biotechnology. This can also redefine the frontiers of sovereignty and also rebrand the measures of power in the twenty first century.

REFERENCES

Abd al-Azim, D. F. J., et al. (2023). The trend of states towards adopting data localisation policies: A study of the concept, motives, conditions, and requirements. *Journal of the Faculty of Politics and Economics, 19*.

Al-Ali, A. Z., & Hamid, A. H. (2022). *Tactics of modern warfare: Cyber security, augmented warfare, and hybrid warfare*. Al-Arabi for Publishing and Distribution.

Al-Damdardash, M. M. (2020). The phenomenon of international economic competition and its reflections on peaceful coexistence with focus on issues of trade and comprehensive development. *Journal of Legal and Economic Research, 32*(1).

Al-Dulaimi, A. A. S. (2025). *The effectiveness of power in international politics and its relation to national sovereignty in light of international variables and globalisation*. Dar al-Mu'taz for Publishing and Distribution.

Al-Madani, R. A. (2021). *Globalisation and its impact on national sovereignty*. Dar al-Jinan for Publishing and Distribution.

Al-Sulaymani, A. H. A. (2022). *Diplomatic immunity: Its applications and international laws*. Al-Masriyya for Publishing and Distribution.

Ali, I. A. (2025). Reshaping the world, rethinking actors: Role of sub-state actors in foreign relations. *Journal of International Studies, 21*(1).

Araya, D., et al. (2023). Geotechnological rivalry in the data economy. *Transformation: Digital Economies & AI, 37*.

Assad, J. M. (2014). *ISIS and the new jihadists*. Dar al-Yaqut for Printing and Publishing.

Blinken, A. J. (2021–2025). *United States international cyberspace and digital policy strategy: Towards an innovative, secure, and rights-respecting digital future*. U.S. Department of State.

Boost, M. (n.d.). Europe needs to decouple from Big Tech USA: Here's 5 ways it can be achieved. *TechRadar*. https://linksshortcut.com/IuUJy

Bouzidi, A. (2021). The conceptual boundaries of the term "competition" in international relations. *Journal of*

Human Sciences, University of the Brothers Mentouri, Constantine, 21(2), 322–323.
Chander, A., & Sun, H. (2023). *Data sovereignty: From the digital silk road to the return of the state*. Oxford University Press.
Chen, J. (2025). Nash equilibrium: How it works in game theory, examples, plus Prisoner's Dilemma. https://share.google/GszQJOtfmI9AQ59eE
Dawood, N. Z., & Jasem, F. H. (2023). The power vacuum and the authority of informal actors. *Russian Law Journal, XI*(8), 170–171.
Digital Samba. (2025). Navigating data sovereignty: Compliance and business impact. https://linksshortcut.com/gfsnF
Fahmi, A. (2022). *Media and the other: Cultural sovereignty and the reinforcement of identities*. Arab Press Agency (Publishers).
Fratini, S., et al. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. *Digital Society*. Springer Nature.
García, C. S. (2024). *Digital expansionism and big tech companies: Consequences in democracies of the European Union*. Universitat Jaume I de Castelló.
Ishkhanyan, A. (2025). The sovereignty–internationalism paradox in AI governance: Digital federalism and global algorithmic control. *Discover Artificial Intelligence*.
Jansen, B., Kadenko, N., et al. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly, 40*(4).
Kadhim, H. A., & Abd, Q. M. (2020). Voting behaviour of permanent members of the Security Council regarding the American war on Iraq in 2003. *Journal of Political Issues, 63*.
Khalaf, H. M. (2024). The methodological and epistemological developments in conflict and peace studies. *Conflict Studies Quarterly, 47*.
Lambach, D., & Oppermann, K. (2022). Narratives of digital sovereignty in German political discourse. *Institute for Political Science, Chemnitz University of Technology*.
Larsen, B. C. (2022). The geopolitics of AI and the rise of digital sovereignty. *Brookings Institution*. https://linksshortcut.com/WuHfX
Lilkov, D. (2023). Technological sovereignty? Delivering a complete European digital single market. *Wilfried Martens Centre for European Studies, 22*(2).
Manati, T. K., & Alwan, S. O. (2024). Transformations of the world order after the COVID-19 pandemic: The role of culture, science, and the environment. *Journal of International Crisis and Risk Communication Research, 7*.
Martynova, E., & Shcherbovich, A. (2024). Digital transformation in Russia: Turning from a service model to ensuring technological sovereignty. *Computer Law and Security Review, 55*, 106075. https://linksshortcut.com/TtEHC
Meneses, M. (2025). Digital sovereignty: Cutting dependence on dominant tech companies. https://linksshortcut.com/OOFpn
Nadhir, H. M. (2014). *The phenomenon of international competition in international relations*. Arab Democratic Centre. https://democraticac.de/?p=1775
Pohle, J. (2020). Digital sovereignty: A new key concept of digital policy in Germany and Europe. *Konrad-Adenauer-Stiftung e. V.*
Roudani, C. (2025). Cyber deterrence and digital resilience: Towards a new doctrine of global defense. *Modern Diplomacy*. https://linksshortcut.com/VuiQs
Saadi, M. (2020). *The impact of new technology on public international law*. Al-Dar al-Masriyya for Publishing and Distribution.
Shoker, A. (2022). Digital sovereignty strategies for every nation. *King Abdullah University of Science and Technology, 1*(1).
State Council Information Office of the People's Republic of China. (2025). *China's national security in the new era*. https://share.google/2Co9HzFxjzUaneVvq
Thumfart, J. (2022). *The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the COVID crisis 2020/21 as catalytic event*. Bloomsbury.
United Nations. (2021). *IGF 2021 WS #106 open source collaboration for digital sovereignty*. https://linksshortcut.com/luzoS
Wu, E. (2021). Sovereignty and data localisation. *Harvard Kennedy School Belfer Center for Science and International Affairs, Harvard University*

.