

Cyberspace Governance Between Sovereignty and Openness: Issues of Digital Governance in Light of International Geopolitical Competition

Noureddine LASSEL

University of Biskra, (Algeria)

Email (noureddine.lassel@univ-biskra.dz)

Received
26/04/2026

Accepted
04/09/2026

Published
31/10/2026

Abstract:

This article examines the tension between digital sovereignty and openness in the governance of cyberspace. Drawing on digital liberalism, cyber realism and constructivism, it explains why the United States, China and the European Union have developed markedly different models of digital governance, and it assesses the capacity of existing legal and institutional regimes -from the World Summit on the Information Society to the Tallinn Manual and the UN Convention against Cybercrime- to regulate a domain that resists territorial logic.

Methodologically, the study combines a descriptive-analytical approach with comparative analysis and the discourse analysis of official state positions. It argues that the fragmentation of the Internet is less a technological necessity than a political choice driven by geopolitical rivalry, and that developing and Arab states bear its costs disproportionately. The article proposes a consensus-based model of digital governance grounded in pluralism, fairness and adaptability, while acknowledging the structural constraints that limit any such model.

Keywords:

Cyberspace Governance - Digital Sovereignty - Digital Governance - Geopolitical Competition - Internet Fragmentation

Introduction:

The emergence and rapid expansion of cyberspace mark a fundamental turning point in contemporary international relations. Cyberspace is not merely a technical infrastructure for the exchange of information; it is a strategic domain in which the interests of state and non-state actors intersect and collide. Within a few decades, a network initially confined to academic and military uses has become a global infrastructure connecting more than five billion people and permeating the economic, political and social structures of states and societies. This transformation poses unprecedented challenges to an international governance system originally designed to regulate a physical world organized around territorial borders and national sovereignty.¹

At the heart of the problem lies a structural contradiction inherent in cyberspace itself. Born of a philosophy of openness and decentralization, the Internet resists the logic of borders and territorial sovereignty; yet states, increasingly alert to the security, economic and political risks it generates, have moved to extend their sovereign instruments into the digital domain in order to contain and control it. Cyberspace has thus become the site of a twofold contest: a normative contest between the paradigms of openness and sovereignty, and a geopolitical contest among major powers seeking to shape its governance in line with their strategic interests.

This tension has surfaced repeatedly in international negotiations on Internet governance: at the World Summit on the Information Society, held in Geneva in 2003 and in Tunis in 2005;² in the recurring controversy over the respective roles of the International Telecommunication Union (ITU) and the Internet Corporation for Assigned Names and Numbers (ICANN); and, more recently, in the United Nations negotiations that culminated in the adoption of the UN Convention against Cybercrime by the General Assembly in December

¹ Laura DeNardis, ed., *The Global War for Internet Governance* (London: Yale University Press, 2014).

² World Summit on the Information Society, “WSIS: Declaration of Principles,” December 12, 2003.

2024.¹ Across these forums, the positions of the main actors diverge sharply. The United States and its Western partners have championed a multistakeholder model in which the private sector and civil society play a leading role and which is framed around the free flow of information, whereas China and Russia have promoted a state-centric model premised on full sovereign control over national digital spaces.

Against this background, the study addresses the following research question: **In light of the rapid development of cyberspace and its transformation into an arena of geopolitical competition, how can states' demands for digital sovereignty be reconciled with the requirements of openness and global Internet governance?**

The study advances three hypotheses. First, intensifying geopolitical competition is pushing states towards increasingly assertive models of digital sovereignty. Second, the absence of a binding international legal framework widens the gap between the competing governance models. Third, developing states, including Arab states, are the most exposed to the costs of this rivalry because of their structural digital dependence.

To test these hypotheses, the study combines three complementary approaches: a descriptive-analytical approach to map the phenomenon and its dimensions; a comparative approach to examine the principal international models of digital governance; and discourse analysis of the official positions that states articulate in international forums. The article proceeds in four sections: the first sets out the theoretical and conceptual framework; the second compares the American, Chinese and European models; the third analyses the crisis of digital governance under conditions of geopolitical rivalry; and the fourth outlines the contours of a consensus-based model of governance.

1. Section I: THEORETICAL AND CONCEPTUAL FRAMEWORK

Any study of cyberspace governance requires a clear theoretical and conceptual framework that defines its key terms and identifies its analytical tools. Conceptual ambiguity in this field frequently leads to confusion between levels of analysis and to overlapping, and at times contradictory, conclusions.

¹ United Nations Office on Drugs and Crime, *NITED NATIONS CONVENTION AGAINST CYBERCRIME*, Global Programme on Cybercrime (Vienna, 2025).

A) The Transition from the Westphalian to the Digital

Concept of Sovereignty:

1- Sovereignty in the Traditional Sense and Its Theoretical Foundations:

Sovereignty is among the oldest and most contested concepts in international political and legal thought. Its modern origins are conventionally traced to the Peace of Westphalia (1648), which consolidated the principles of the legal equality of states and of each state's exclusive authority within its territory, free from external interference.¹ Jean Bodin's earlier definition of sovereignty as the absolute and perpetual power of the state over its subjects and territory provided a durable reference point for international legal thought for several centuries.

Classical sovereignty rests on three interdependent elements: a territory delimited by internationally recognized borders, a permanent population subject to the state's authority, and a government capable of exercising effective control. The 1933 Montevideo Convention on the Rights and Duties of States added a fourth criterion of statehood: the capacity to enter into relations with other states.²

2- Concept and Dimensions of Digital Sovereignty

Digital sovereignty is a relatively recent concept that has gained currency in political and scholarly debate since the early twenty-first century, and especially over the past decade. In essence, it denotes a state's capacity to exercise effective control over the digital infrastructure, data flows and technologies that operate within its jurisdiction, and to make autonomous decisions in digital policy free from external constraints.³

Digital sovereignty can be analysed along four interrelated dimensions: a technical dimension, concerning control over infrastructure, networks and technical standards; a legal dimension, concerning the capacity to regulate digital activities and to enforce national law in cyberspace; an economic dimension, concerning the

¹ Leo Gross, "The Peace of Westphalia, 1648–1948," *American Journal of International Law* 42, no. 1 (1948): 20–41.

² United States of America and Cuba, "Montevideo Convention on the Rights and Duties of States," December 26, 1933.

³ Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *Philosophy & Technology* 33, no. 3 (2020): 369–78.

development of national digital industries and the reduction of dependence on foreign providers; and a security dimension, concerning the protection of critical information infrastructure and sensitive data against espionage and external intrusion.

B) Theoretical Explanations of Governance in Cyberspace

1- Digital Liberalism and the Philosophy of Openness

Digital liberalism draws on the intellectual heritage of liberal thought in international relations. It regards the Internet, with its decentralized and borderless architecture, as a global commons that should be governed through participatory, multistakeholder arrangements rather than controlled by individual states. From this perspective, the free flow of information is both a condition of economic prosperity and a vehicle for the diffusion of liberal values.¹

2- Cyber Realism and Power Politics

Cyber realism, by contrast, builds on the core tenets of the realist tradition. It holds that states remain the principal actors in the international system and that cyberspace, far from being an exception, is a new extension of the arenas of strategic competition among them. States therefore seek to accumulate cyber capabilities, to deter adversaries and to shape the rules of the domain in accordance with their national interests. Although Joseph Nye writes from a liberal rather than a realist perspective, his analysis of cyber power offers an important qualification: **power in cyberspace remains unevenly distributed, and the reduction of power differentials does not amount to power equalization.**² Governments remain the strongest actors, but power is increasingly diffused to nonstate actors, complicating a purely state-centric reading of the domain.³

3- Constructivism and the Digital Actors' Identity

Constructivism offers a third lens, focusing less on material interests and the balance of power than on identities, ideas and norms. Finnemore and Hollis show that norms for cybersecurity are not given but constructed through processes involving states, firms and other actors, and that their content and legitimacy depend on the social

¹ Milton Mueller, *Networks and States: The Global Politics of Internet Governance*, Information Revolution and Global Politics (Cambridge, Mass: MIT Press, 2010), 264–66.

² Joseph S. Nye, *The Future of Power*, 1st ed (New York: PublicAffairs, 2011), 133–37.

³ Nye, *The Future of Power*, 151.

context in which they emerge.¹ From this perspective, the divergence between the American and Chinese models of digital governance reflects not only different strategic objectives but also different conceptions of the relationship between the state, the individual and information.

C) International Legal and Institutional Regimes

1- The Institutional Setting of Internet Governance

Internet governance is dispersed across a complex array of institutions with distinct and sometimes overlapping mandates. The most prominent is ICANN, which coordinates the Domain Name System and the allocation of Internet Protocol addresses. Established in 1998 as a private non-profit corporation under an agreement with the US Department of Commerce, ICANN long remained the focus of controversy over US oversight.² That oversight formally ended in 2016, when stewardship of the IANA functions was transferred to the global multistakeholder community.

2- The WSIS Process and the International Legal Frameworks

The World Summit on the Information Society (WSIS), held in two phases in Geneva (2003) and Tunis (2005), remains the most ambitious coordinated effort to build a global consensus on the principles of digital governance.³ Its outcomes, including a working definition of Internet governance and the creation of the Internet Governance Forum, institutionalized the multistakeholder principle while leaving the underlying disputes over state authority unresolved.⁴

3- Difficulties in Applying International Law to Cyberspace

The application of international law to cyberspace raises complex problems that remain unresolved. The most serious is attribution: establishing, with sufficient legal and technical certainty, which state or actor is responsible for a cyber operation when perpetrators deliberately conceal their identity. Further difficulties concern the threshold at which a cyber operation amounts to a use of force or an armed attack, and the application of the principles of sovereignty and non-intervention to operations below that threshold. The Tallinn Manual

¹ Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *The American Journal of International Law* 110, no. 3 (2016): 425–79.

² DeNardis, *The Global War for Internet Governance*, 55.

³ World Summit on the Information Society, "WSIS: Declaration of Principles."

⁴ World Summit on the Information Society, "WSIS: Declaration of Principles."

2.0, prepared by an international group of experts, is one of the most comprehensive scholarly attempt to set out how existing international law applies to cyber operations in both peacetime and armed conflict; it remains, however, a non-binding expert restatement rather than an agreed interstate instrument.¹

Section II: Models of Digital Governance in International Practice

This section examines the three principal models that shape the contemporary landscape of global digital governance: the American model, based on openness and private-sector leadership; the Chinese model, based on comprehensive digital sovereignty; and the European model, which seeks a third way between the two.

A) The American Model: Openness Driven by the Private Sector

1- The Historical and Philosophical Foundations of the American Model

The American approach to Internet governance is rooted in the technical culture in which the Internet was born. When the network became a global phenomenon in the 1990s, successive US administrations opted for a strategy that assigned the private sector the leading role in its development and management, while limiting government intervention to securing a predictable legal environment for electronic commerce.²

2- The Role of Big Tech Companies in Digital Governance

The American model has produced a digital order dominated by a small number of large technology corporations, commonly referred to by the acronym GAFAM (Google, Apple, Facebook/Meta, Amazon and Microsoft). These firms not only control much of the infrastructure and many of the services on which billions of users depend, but also exercise quasi-regulatory power through their terms of service and content-moderation policies. Their business models rest on the extraction and monetization of data, a structure that Srnicek characterizes as platform capitalism.³

¹ Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2017), 1–3.

² Tip House, “A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE,” *Profit over Privacy*, 2021.

³ Laurent De Sutter, *Platform Capitalism, Theory Redux*, ed. Nick Srnicek (Cambridge, UK ; Malden, MA: Polity, 2017), pp 6, 44-47.

3- The Constraints of the American Model and Its Internal Contradictions

Although it is framed in the language of openness, the American model has attracted strong criticism that exposes its internal contradictions. The documents disclosed by Edward Snowden in 2013 revealed that the US National Security Agency conducted large-scale electronic surveillance programmes targeting foreign nationals and the leaders of allied states.¹ These revelations undermined the credibility of the US discourse on Internet freedom and strengthened the arguments of states calling for greater digital sovereignty.

B) The Chinese Model – Sovereignty in the Digital Age

1- The Chinese Vision: The Idea of Cyber Sovereignty

China promotes its vision of digital governance under the banner of ‘cyber sovereignty’. According to this principle, each state has the right to govern its national cyberspace in accordance with its own laws, values and objectives, without external interference, and states rather than private or civil-society actors should occupy the central place in international Internet governance.²

2- The Digital Control Infrastructure and the Great Firewall

The most visible component of the Chinese model is the so-called Great Firewall, a complex technical and administrative system through which the state regulates the flow of information across its national borders. Roberts shows that Chinese information control relies less on outright prohibition than on friction and flooding, which raise the cost of accessing undesirable information and dilute it with state-sponsored content.³ Behind this protective barrier, China has developed an integrated national digital ecosystem serving more than one billion users.

3- The Digital Silk Road and the Export of the Chinese Model

The Chinese model is not confined to the domestic sphere. Through the Digital Silk Road, the technological dimension of the Belt and Road Initiative, China exports digital infrastructure -fibre-optic networks,

¹ Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, First Edition (New York, NY: Metropolitan Books/Henry Holt, 2014), pp 126-142.

² Rogier Creemers, “China’s Approach to Cyber Sovereignty,” Berlin: Konrad-Adenauer-Stiftung, 2020, pp 10-11.

³ Margaret E. Roberts, *Censored: Distraction and Diversion inside China’s Great Firewall* (Princeton, New Jersey: Princeton University Press, 2018), pp 5-6, 42-44.

telecommunications equipment, data centres and smart-city systems—and, with them, technical standards and governance practices, particularly in Asia, Africa and the Middle East.¹

C) The European Model: Regulatory Sovereignty and the Third Way

1- Digital Governance Philosophy of the European Union

The European model rejects the wholesale adoption of either the American or the Chinese approach and seeks a third way resting on three pillars: the protection of the fundamental rights of individuals in the digital sphere, the regulation of the market power of large technology platforms, and the development of European strategic autonomy in digital technologies.

2- The General Data Protection Regulation (GDPR) and Its International Impact

The General Data Protection Regulation (GDPR), in force since 2018, is arguably the most influential piece of digital legislation adopted anywhere in recent years. It has compelled major technology companies to redesign their data-handling practices in order to comply with European standards and has inspired similar legislation in numerous jurisdictions. Bradford describes this phenomenon as the ‘Brussels Effect’: the capacity of the EU to shape global markets unilaterally through its regulatory standards.²

3- The Digital Markets Act, the Digital Services Act and Technological Sovereignty

To consolidate its digital sovereignty, the EU adopted the Digital Markets Act (DMA) and the Digital Services Act (DSA) in 2022. The former imposes ex ante obligations on large ‘gatekeeper’ platforms in order to ensure contestable and fair digital markets³ while the latter establishes a framework of accountability for online intermediaries,

¹ Jonathan E. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (New York: Harper Business, 2021), chap 7.

² Anu Bradford, *The Brussels Effect The Brussels Effect How the European Union Rules the World*, 1st ed. (Oxford University Press New York, 2020), pp 2,25-26.

³ European Union, “Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act),” in *Official Journal of the European Union*, L 265, October 12, 2022, 1–66.

including enhanced obligations for very large online platforms.¹ Together, they constitute an unprecedented regulatory framework for curbing the market dominance of large technology firms in the European digital market.

Section III: The Crisis of Digital Governance and Geopolitical Competition

Great-power competition is no longer confined to the traditional military, economic and diplomatic domains. It has extended into the digital sphere, a new strategic arena in which the interests of states intersect and their competing visions of the future international order collide.

A) Internet Fragmentation and the ‘Splinternet’

1- The Concept of Digital Fragmentation and Its Genesis

In recent years, the global digital space has witnessed an accelerating trend towards what the academic and policy literature terms the ‘splinternet’-a portmanteau of ‘splinter’ and ‘Internet’-denoting the gradual fragmentation of a single, open global network into multiple, partially disconnected digital spaces. Drake, Cerf and Kleinwächter distinguish three forms of this process: technical fragmentation; governmental fragmentation, driven by state policies; and commercial fragmentation, driven by corporate practices.²

2- Contemporary Manifestations of Fragmentation

Fragmentation is visible in several concrete developments. The first is the spread of data localization requirements, which oblige firms to store or process certain categories of data within national borders: by early 2023, the OECD had identified 100 such measures in force across 40 countries, more than two-thirds of which combined local storage requirements with restrictions on cross-border transfers.³ The second is the growing politicization of cross-border data flows in development and trade policy.⁴ The third is competition over technical standards,

¹ European Union, “Single Market for Digital Services and Amending Directive,” in *Official Journal of the European Union*, no. 2022/2065, L 277 (2022), 1–102.

² William J. Drake et al., *Internet Fragmentation: An Overview*, Future of the Internet Initiative White Paper (Geneva: World Economic Forum, 2016), pp 14–15.

³ Chiara el Giovane et al., *The Nature, Evolution and Potential Implications of Data Localisation Measures*, OECD Trade Policy Papers no. 278, OECD Trade Policy Papers (2023), 13.

⁴ United Nations, *Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow*, UNCTAD/DER/2021, Digital Economy Report (Geneva: United Nations, 2021).

exemplified by the rivalry between the United States and its allies, on the one hand, and China, on the other, over 5G networks.

3- Strategic Implications of Internet Fragmentation

The consequences of fragmentation extend well beyond the technical sphere and affect the architecture of the international system as a whole. Economically, data localization raises operating costs for firms and their downstream users and may, paradoxically, increase vulnerability to fraud and cybersecurity risks while reducing resilience to unexpected shocks.¹ Politically, fragmentation entrenches competing spheres of digital influence and weakens the prospects for universal rules.

B) Arab and Developing Countries Between Two Digital Poles

1- The Digital Dependency Question in the Global South

Countries of the Global South frequently experience digital dependence at three interrelated levels: technological dependence on foreign hardware, software and infrastructure; data dependence, as the data generated by their populations are stored and processed abroad; and regulatory dependence, as they adopt rules designed elsewhere. Kwet conceptualizes this configuration as digital colonialism: the structural control exercised by dominant, predominantly US-based technology corporations over the digital ecosystem of the Global South—its software, hardware and network connectivity.²

2- Arab Positions in International Digital Governance Platforms

Arab positions on Internet governance, as expressed in international forums, have tended to be fragmented and inconsistent, reflecting the political and economic disparities within the region. This fragmentation points to the absence of a coherent Arab digital strategy and to a shortage of specialized expertise capable of engaging effectively in highly technical legal and policy negotiations.³

3- The Digital Divide and the Question of Equity in Governance

The North–South digital divide remains one of the most profound problems of global digital governance and one of the principal challenges to international justice. The question of justice in digital governance has several dimensions, of which three are central:

¹ el Giovane et al., *The Nature, Evolution and Potential Implications of Data Localisation Measures*.

² Michael Kwet, “Digital Colonialism: US Empire and the New Imperialism in the Global South,” *Race & Class* 60, no. 4 (2019): 3–26.

³ Internet Governance Forum, “Arab Regional Internet Governance Forum,” 2023.

representative justice, concerning participation in rule-making institutions; distributive justice, concerning access to digital resources and their benefits; and procedural justice, concerning the fairness of decision-making processes. Countries of the South are frequently disadvantaged on all three dimensions simultaneously.

C) Non-State Actors and the Reshaping of Governance

1- Technology Companies as Geopolitical Actors

Major technology companies now exercise a geostrategic influence that, in certain respects, rivals that of sovereign states. This influence operates through three simultaneous channels: control over critical infrastructure, such as cloud services and submarine cables; control over the circulation of information through search engines, social media and content moderation; and a form of private digital diplomacy, through which firms negotiate directly with governments and international organizations.

2- Digital Civil Society and Pressure on the Governance System

Digital civil society has become an increasingly important actor in the governance ecosystem. It encompasses a broad spectrum of non-governmental organizations, human rights groups and digital rights activists. Organizations such as the Electronic Frontier Foundation (EFF) and Access Now have played a key role in documenting violations of digital rights and in holding both governments and companies to account, for instance by publicly assessing how firms respond to government requests for user data.¹

3- Artificial Intelligence and the New Frontier of Geopolitical Competition

Artificial intelligence (AI) opens a new chapter in the geopolitics of the digital domain, one whose stakes may exceed those of earlier struggles over control of the Internet. AI is not merely another technology: Horowitz argues that it resembles general-purpose enabling technologies such as electricity or the combustion engine more than a specific weapon, and that its effects on military power and the balance of power will depend largely on how states and organizations adopt it.² Competition over AI capabilities, computing power and the

¹ Electronic Frontier Foundation, “Who Has Your Back? Protecting Your Data from Government Requests,” 2022.

² Michael C. Horowitz, “Artificial Intelligence, International Competition, and the Balance of Power,” *Texas National Security Review* 1, no. 3 (2018): 36–57.

rules governing AI is therefore becoming a central dimension of great-power rivalry.

Section IV: Towards a Consensus-Based Model of Digital Governance

This final section addresses the most pressing and difficult question raised by the analysis: how can a consensus-based model of digital governance be constructed that transcends the dichotomy between sovereignty and openness, acknowledges the plurality of actors and their conflicting interests, and establishes fair and sustainable rules for the governance of global cyberspace?

A) Review of Existing Models and Lessons Learned

1- Parameters for Evaluating Digital Governance Models

This study proposes five integrated criteria for evaluating existing models of digital governance: effectiveness, legitimacy, fairness, adaptability and accountability. Assessed against these criteria, each model satisfies some requirements at the expense of others: the American model performs well on adaptability but poorly on accountability; the Chinese model is effective in terms of state control but weak on legitimacy and fairness beyond its borders; and the European model scores highly on accountability and rights protection but less so on technological capacity.

2- Shortcomings of the Current Governance System

The existing international framework of digital governance suffers from structural deficiencies that prevent it from performing its intended functions. Three stand out: institutional fragmentation across multiple forums with overlapping mandates; the widening gap between the pace of technological change and the slowness of institutional adaptation; and the lack of enforcement mechanisms, which leaves most declarations and recommendations dependent on the voluntary compliance of the most powerful actors.

3- International Experiences and Lessons

Comparative international experience offers several lessons. First, the European experience suggests that stringent regulation need not stifle digital innovation. Second, multistakeholder forums show that a richer and more inclusive deliberation becomes possible when governments, the private sector and civil society are brought together within a single consultative framework, even where such forums lack decision-making authority.

B) Recommendations for a Just Digital Governance Framework

1- Principles of Good Digital Governance

Any consensus-based model for the governance of the digital space should rest on four core principles: pluralism in representation, balance between rights and responsibilities, transparency in decision-making, and responsiveness to technological change.

2- Towards an International Cyberspace Treaty

One of the most contested proposals is a comprehensive international treaty on cyberspace. This study advocates an incremental path: rather than seeking a single comprehensive instrument, states could build a layered regime of narrower, sector-specific agreements - such as a convention prohibiting cyberattacks against critical civilian infrastructure- that could gradually converge towards a more comprehensive framework. The adoption of the UN Convention against Cybercrime in 2024, despite the controversy surrounding its human rights safeguards, indicates that such sectoral agreements remain attainable [3].

3- Reforming Multilateral Governance Institutions

A fairer model of digital governance requires substantive reform of existing institutional arrangements. ICANN, in particular, should strengthen the representation of countries of the Global South in its decision-making structures and limit the disproportionate influence of multinational corporations.

C) The Position of Arab Countries in the Future of Digital Governance

1- Current Challenges Facing Arab Digital Governance

Arab countries face a complex set of challenges that limit their capacity to participate effectively in the governance of the digital space: a persistent digital divide, political fragmentation, the absence of a unified Arab digital strategy, and an internal tension between efforts to pursue digital transformation for development and policies aimed at controlling the flow of information.

2- Available Opportunities and Untapped Assets

Despite these challenges, the Arab region possesses significant untapped assets: a large and predominantly young population, a strategic location at the crossroads of major international submarine cable routes, and the substantial financial resources of the Gulf states.

3- Towards an Independent Arab Digital Strategy

The proposed Arab digital strategy rests on five interrelated pillars: coordinated Arab positions in international forums; the development of specialized human capital; the harmonization of digital legislation; investment in regional digital infrastructure; and support for Arab digital innovation and entrepreneurship.

Conclusion

This study set out to examine how states' claims to digital sovereignty can be reconciled with the requirements of openness and global Internet governance amid intensifying geopolitical competition in cyberspace. The analysis developed across the four sections points to an answer that does not side with either pole of this dichotomy but seeks to move beyond it towards a more realistic and equitable settlement.

First: Key Findings

At the conceptual level, the study has shown that digital sovereignty is not a mere extension of Westphalian sovereignty but a distinct concept whose technical, legal, economic and security dimensions are closely intertwined. At the level of practice, each of the three major models displays its own internal contradictions: the American model, while advocating openness, is not free of a hegemonic strategic agenda; the Chinese model, while insisting on full sovereignty, exports practices of surveillance and control; and the European model, despite its leadership in the protection of digital rights, is constrained by limited technological capabilities.

From a geopolitical perspective, the fragmentation of the Internet is not a technological necessity but essentially a political choice, reflecting deeper fractures in an international order undergoing profound change. The study has further shown that developing countries, and Arab countries in particular, are among those most exposed to the costs of this digital rivalry.

Second: Testing Hypotheses

The findings lend support to the study's three hypotheses, albeit to varying degrees. The first hypothesis, concerning the effect of intensifying geopolitical competition on models of digital sovereignty, is clearly confirmed. The second, which holds that the absence of a binding legal framework widens the gap between the competing models, is also confirmed. The third, concerning the position of developing countries, is confirmed with an important qualification:

their dependence is not absolute, and it leaves room for agency through regional coordination and selective partnerships.

Third: Tackling the Core Problem

The answer to the central research question is that reconciling digital sovereignty with openness is not a diplomatic aspiration but a strategic necessity imposed by the logic of global interdependence. Such reconciliation, which is both feasible and desirable, requires neither the abolition of digital sovereignty nor the sacrifice of openness, but a redefinition of both in the light of the principles of fairness, multilateralism and shared responsibility.

Ultimately, cyberspace mirrors the international community, reflecting both its contradictions and its aspirations. If the international system moves towards greater cooperation and solidarity, digital governance can rest on consensus; if tendencies towards rivalry and closure prevail, cyberspace will become increasingly fragmented and less able to serve humanity as a whole.

Fourth: Research Prospects and Recommendations for Future Research

The study opens several avenues for future research. The international governance of artificial intelligence warrants a dedicated, in-depth study. Digital governance in the Arab region remains an under-researched field that calls for specialized empirical work. Finally, comparative analysis of Arab digital legislation would help to trace its evolution and identify existing gaps.

Bibliography

- 1 - Bradford, Anu. *The Brussels Effect The Brussels Effect How the European Union Rules the World*. 1st ed. Oxford University Press New York, 2020.
- 2 - Creemers, Rogier. "China's Approach to Cyber Sovereignty." Berlin: Konrad-Adenauer-Stiftung, 2020.
- 3 - De Sutter, Laurent. *Platform Capitalism*. Theory Redux, edited by Nick Srnicek. Cambridge, UK ; Malden, MA: Polity, 2017.
- 4 - DeNardis, Laura, ed. *The Global War for Internet Governance*. London: Yale University Press, 2014.
- 5 - Drake, William J., Vinton G. Cerf, and Wolfgang Kleinwächter. *Internet Fragmentation: An Overview*. Future of the Internet Initiative White Paper. Geneva: World Economic Forum, 2016.

- 6 - Electronic Frontier Foundation. "Who Has Your Back? Protecting Your Data from Government Requests." 2022.
- 7 - European Union. "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)." In *Official Journal of the European Union*, L 265, 1–66. October 12, 2022.
- 8 - ———. "Single Market for Digital Services and Amending Directive." In *Official Journal of the European Union*, No. 2022/2065, L 277, 1–102. 2022.
- 9 - Finnemore, Martha, and Duncan B. Hollis. "Constructing Norms for Global Cybersecurity." *The American Journal of International Law* 110, no. 3 (2016): 425–79.
- 10 - Floridi, Luciano. "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *Philosophy & Technology* 33, no. 3 (2020): 369–78.
- 11 - Giovane, Chiara el, Janos Ferencz, and Javier López-González. *The Nature, Evolution and Potential Implications of Data Localisation Measures*. OECD Trade Policy Papers No. 278. OECD Trade Policy Papers. 2023.
- 12 - Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. First Edition. New York, NY: Metropolitan Books/Henry Holt, 2014.
- 13 - Gross, Leo. "The Peace of Westphalia, 1648–1948." *American Journal of International Law* 42, no. 1 (1948): 20–41.
- 14 - Hillman, Jonathan E. *The Digital Silk Road: China's Quest to Wire the World and Win the Future*. New York: Harper Business, 2021.
- 15 - Horowitz, Michael C. "Artificial Intelligence, International Competition, and the Balance of Power." *Texas National Security Review* 1, no. 3 (2018): 36–57.
- 16 - House, Tip. "A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE." *Profit over Privacy*, 2021.
- 17 - Internet Governance Forum. "Arab Regional Internet Governance Forum." 2023.
- 18 - Kwet, Michael. "Digital Colonialism: US Empire and the New Imperialism in the Global South." *Race & Class* 60, no. 4 (2019): 3–26.

- 19 - Mueller, Milton. *Networks and States: The Global Politics of Internet Governance*. Information Revolution and Global Politics. Cambridge, Mass: MIT Press, 2010.
- 20 - Nye, Joseph S. *The Future of Power*. 1st ed. New York: PublicAffairs, 2011.
- 21 - Roberts, Margaret E. *Censored: Distraction and Diversion inside China's Great Firewall*. Princeton, New Jersey: Princeton University Press, 2018.
- 22 - Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press, 2017.
- 23 - United Nations. *Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow*. UNCTAD/DER/2021. Digital Economy Report. Geneva: United Nations, 2021.
- 24- United Nations Office on Drugs and Crime. *NITED NATIONS CONVENTION AGAINST CYBERCRIME*. Global Programme on Cybercrime. Vienna, 2025.
- 25 - United States of America, and Cuba. "Montevideo Convention on the Rights and Duties of States." December 26, 1933.
- 26 - World Summit on the Information Society. "WSIS: Declaration of Principles." December 12, 2003.