Advances in Science, Technology & Innovation
IEREK Interdisciplinary Series for Sustainable Development

Haitham M. Alzoubi · Anwar S. Al-Gasaymeh · Srinidhi Vasudevan *Editors*

Bridging Digital Innovation and Technology for Business Transformation—ICTIM

IEREK RESEARCH & KNOWLEDGE ENRICHMENT

Springer

Advances in Science, Technology & Innovation

IEREK Interdisciplinary Series for Sustainable Development

Advances in Science, Technology & Innovation (ASTI) is a series of peer-reviewed books based on important emerging research that redefines the current disciplinary boundaries in science, technology and innovation (STI) in order to develop integrated concepts for sustainable development. It not only discusses the progress made towards securing more resources, allocating smarter solutions, and rebalancing the relationship between nature and people, but also provides in-depth insights from comprehensive research that addresses the **17 sustainable development goals (SDGs)** as set out by the UN for 2030.

The series draws on the best research papers from various IEREK and other international conferences to promote the creation and development of viable solutions for a **sustainable future and a positive societal** transformation with the help of integrated and innovative science-based approaches. Including interdisciplinary contributions, it presents innovative approaches and highlights how they can best support both economic and sustainable development, through better use of data, more effective institutions, and global, local and individual action, for the welfare of all societies.

The series particularly features conceptual and empirical contributions from various interrelated fields of science, technology and innovation, with an emphasis on digital transformation, that focus on providing practical solutions to **ensure food, water and energy security to achieve the SDGs.** It also presents new case studies offering concrete examples of how to resolve sustainable urbanization and environmental issues in different regions of the world.

The series is intended for professionals in research and teaching, consultancies and industry, and government and international organizations. Published in collaboration with IEREK, the Springer ASTI series will acquaint readers with essential new studies in STI for sustainable development.

ASTI series has now been accepted for Scopus (September 2020). All content published in this series will start appearing on the Scopus site in early 2021.

Conceptual and Legal Issues for National Cyber Sovereignty

Mahmoud Ismail, Noor Saleh Ali Alzyoud, Fayez A. L. Nusair, and Randa E. L. Hasi

Abstract

The research delves into the intricate legal hurdles posed by cyberspace to the notion of sovereignty in both international and national legal frameworks, highlighting two pivotal aspects: issues stemming from the essence of sovereignty and those arising during its practical enforcement. Cyberspace introduces legal complexities to state sovereignty, given its inherent openness, which stands in stark contrast to the traditional closed nature prerequisite for sovereignty. The phenomenon of globalization exacerbates these complexities, as transnational governmental bodies and communities endeavor to leverage cyberspace for economic and cultural pursuits, thereby intensifying the clash between sovereignty and the inherent openness of cyberspace. The delineation of cyber sovereignty necessitates a delicate equilibrium between the principles of sovereignty and the unique characteristics of cyberspace to uphold their respective identities. A nuanced understanding of cyber sovereignty aids in delineating the actual scope of state jurisdiction in governing and regulating cyberspace, thereby addressing the legal dilemmas confronted by states in this domain. The research concludes that cyber sovereignty embodies an application of sovereignty in its conventional sense, rather than a mere synonymous concept. It advocates for international acknowledgment of this novel application and advocates for collaborative endeavors aimed at its regulation to tackle emergent issues in cyberspace, ensuring global security and stability.

Keywords

Cyber sovereignty · Legal concepts · National law

1 Introduction

The advent of the cyber environment introduces intricate legal hurdles to state sovereignty, arising from the fundamental clash between the openness inherent in cyberspace and the closed structure demanded by traditional sovereignty. These issues emerge within the contemporary legal discourse amidst the backdrop of globalization, where supra-governmental entities pursue profit and market exploitation, juxtaposed with societies utilizing cyberspace for communication and cultural exchange (Adams & Albakajai, 2016).

Yet, this very openness also unleashes threats transcending borders, impacting both state frameworks and societal norms. The crux of the matter lies in the borderless nature of cyberspace. Despite technology's primary impetus being commerce rather than politics, one can argue that the original architects of internet technology were influenced by a political agenda aimed at accommodating capitalist interests. Their aim was to curtail state authority by establishing a decentralized network that interconnected the globe without a central controlling node (Schneider, 2013). However, cyberspace has substantially diminished the role of states in regulating interactions within it.

This predicament prompts inquiries into the scope and essence of international sovereignty in an increasingly interconnected world, underscoring the imperative to define the actual reach of state authority in regulating cyberspace within national borders. Achieving this necessitates a meticulous definition of cyber sovereignty, striking a delicate balance

M. Ismail (✉)
Applied Science Private University, Amman, Jordan
e-mail: m_turabi@asu.edu.jo

N. S. A. Alzyoud
Philadelphia University, Amman, Jordan

F. A. L. Nusair
Al Ain University, Abu Dhabi, United Arab Emirates

R. E. L. Hasi
AL Zarka University, Zarqa, Jordan

H. M. Alzoubi et al. (eds.), *Bridging Digital Innovation and Technology for Business Transformation—ICTIM*,
Advances in Science, Technology & Innovation, https://doi.org/10.1007/978-3-031-90558-2_25

between the principles of sovereignty and the unique attributes of cyberspace to preserve the integrity of both concepts.

Kuehl (2009) delineates cyberspace as a global domain within the informational environment, characterized by its distinctive attributes shaped by electronics and the electromagnetic spectrum, facilitating the creation, storage, modification, exchange, and exploitation of information across interconnected networks using communication and information technologies. Meanwhile, sovereignty remains a steadfast concept in the contemporary international system, closely intertwined with the notion of the state as a distinct regional entity, granting it membership within the international order. Any erosion of state sovereignty within the traditional paradigm would precipitate the disintegration of the international community itself, thereby weakening its functionality.

2 Issues Associated with the Concept of Cyber Sovereignty

Legal concepts serve as the foundation of legal systems, delineating their boundaries and operational frameworks. These concepts are pivotal for the interpretation, comprehension, and application of laws by legal practitioners, judges, and law enforcement agencies. Therefore, addressing the conceptual issues posed by cyberspace to the notion of sovereignty is essential.

Defining the parameters of sovereignty in international law can be intricate due to its multifaceted nature. Sovereignty encompasses both internal and external dimensions of state authority. Internally, it delineates the powers of public authority and its capacity to regulate within state borders, while externally, it determines a state's interactions with other entities in the international arena.

Krasner (1999) offers a comprehensive framework for understanding sovereignty, categorizing it into four distinct dimensions: internal sovereignty, reciprocal sovereignty, legal international sovereignty, and Westphalian sovereignty. These classifications provide theoretical components for dissecting the concept of sovereignty. However, for the purpose of discussing cyber sovereignty, we simplify these classifications into two: internal sovereignty, pertaining to the relationship between the state authority and its citizens, and international sovereignty, referring to the state's interactions with the global community.

The cyber environment influences internal sovereignty by challenging the state's control over external influences on societal harmony via the internet. Similarly, international sovereignty is impacted when external influences, facilitated by cyberspace, result from deliberate interference by one state in the affairs of another.

The concept of cyber sovereignty presents two primary issues to the established concept of sovereignty in legal jurisprudence. Firstly, distinguishing between the two concepts, which, despite their similarities, are distinct entities. While there are points of convergence, they are not interchangeable but rather complementary (Al-Gharaibeh et al., 2023). Secondly, cyberspace's impact on sovereignty alters the traditional elements upon which sovereignty relies. Whereas traditional sovereignty emphasizes institutional power, cyber sovereignty necessitates the empowerment of individuals.

2.1 Comparing Cyber Sovereignty with Traditional Sovereignty

Is cyber sovereignty synonymous with traditional sovereignty? Addressing this question is essential before delving into the legal issues of cyber sovereignty in international and national law, as subsequent discussions will draw upon the elements and terminology of traditional sovereignty.

Upon analysis, it becomes evident that cyber sovereignty and traditional sovereignty are not identical in meaning. Traditional sovereignty encompasses a broader scope and implementation than cyber sovereignty (Bu et al., 2023). While traditional sovereignty denotes a state's supreme authority over its territory, population, and governance, as well as its ability to legislate and enforce laws within its borders, cyber sovereignty is confined to a state's jurisdiction over activities within its cyber domain, including online networks and data flow. It operates solely within the virtual realm.

Furthermore, traditional sovereignty's scope extends to a state's authority over physical territory, encompassing governance, law enforcement, defense, and international relations, whereas cyber sovereignty is limited to the virtual realm within a state's borders (Eli, 2022). Although borders remain relevant in cyber sovereignty, their significance diminishes in a borderless cyber environment.

In terms of control and regulation, traditional sovereignty involves governance through established legal and political institutions, exerting tangible control over physical territories, borders, and populations. In contrast, cyber sovereignty entails control over the cyber domain through regulatory frameworks, laws, and technical measures, such as cyber laws, regulations, and collaboration with internet service providers and technology companies.

Moreover, the nature of disputes faced by states differs between traditional and cyber sovereignty. Traditional sovereignty entails regional conflicts, border security issues, and external threats, while cyber sovereignty involves cybersecurity threats and disputes over internet governance.

Additionally, the parties involved in traditional sovereignty are states and international institutions, whereas in cyber sovereignty, the predominant actors are private sector companies and entities.

Lastly, traditional sovereignty is supported by established legal principles and international treaties regulating state behavior and relations, whereas cyber sovereignty requires the development of new legal and political frameworks tailored for the cyber domain, including data protection laws and international agreements on cyber standards (Guergov, 2021).

In summary, while traditional sovereignty encompasses a state's authority over its territory, population, and governance, cyber sovereignty pertains to a specific aspect of state authority within the cyber domain. Discussions on the concept, scope, and implementation of cyber sovereignty in international and national law will undoubtedly be framed within the context of traditional sovereignty, as recognized by international agreements and national laws extending sovereignty to cyberspace regulation, addressing issues such as internet governance, law enforcement, and international cooperation.

2.2 Evolving Dynamics of Sovereignty: Shifting from Authority to the People's Power

Sovereignty is vital for state formation, combining elements of territory and populace. It serves as a bulwark safeguarding independence and identity against external influences (Ong, 2012). However, the relationship between the people, as the source of authority, and the state institutions representing them, is intricate. The people precede the state and are its ultimate objective, while the state serves as a means to their ends. This dynamic engenders tension and attraction between the people and sovereignty, ultimately resolved through societal consensus achieved via legislative mechanisms.

Stable legal frameworks confer legitimacy upon state institutions to exercise sovereignty over the people, represent them internationally, and safeguard their interests. However, these frameworks are susceptible to power dynamics and control over time, which are inherent to the concept of sovereignty (Hinsley, 1967). The emergence of cyberspace introduces a novel dynamic, allowing for connectivity and influence outside traditional power structures.

Foucault (1980) posits that sovereignty's realization extends beyond the legitimacy of restraint and accountability to encompass the management of knowledge and information. Cyberspace, by its very nature, issues sovereignty by democratizing access to information and disrupting traditional power dynamics. This antagonistic relationship between information and control reveals that those who control information wield power, while widespread dissemination of information diminishes control.

This dynamic also applies to knowledge, albeit with a long-term and profound impact compared to information's immediate effect. In the realm of cyber sovereignty, questions arise regarding individuals' consent to state intervention in online activities, the boundaries of state authority in cyberspace regulation, and individuals' rights and responsibilities in the digital age.

Foucault's insights into knowledge and power challenge traditional notions of state authority. His concept of governmentality highlights how institutions employ techniques and strategies to govern populations (Foucault, 1980). Power, as a tool for exercising sovereignty, operates not only through coercion but also through knowledge and discourse.

The flow of information from cyberspace disrupts traditional power structures, compelling states to adapt to the evolving landscape. Some, like China, isolate their citizens from the global cyberspace to retain control. However, this poses a challenge to state authority, as the democratization of information empowers individuals to challenge existing power structures.

The convergence of cyberspace and sovereignty issues traditional notions of state control and authority. It partially shifts power from state institutions to individuals, blurring the lines between traditional sovereignty and the people's power. In this paradigm, individuals become active participants in shaping societal and political discourse, bypassing traditional power structures.

In conclusion, sovereignty transcends mere political control, intertwining with knowledge, discourse, and societal values. Cyberspace disrupts traditional power dynamics, empowering individuals and challenging state authority. This shift towards people's sovereignty redefines the concept of sovereignty itself, as individuals become active agents in shaping governance and societal norms, independent of traditional power structures.

3 Issues in Implementing Cyber Sovereignty

When applying the concept of cyber sovereignty to real-world scenarios, parallels with traditional sovereignty emerge. Traditional sovereignty grants states exclusive authority and control over their physical territories, including land, air, and territorial waters. International law recognizes territorial sovereignty, allowing states to govern within their borders without external interference.

However, applying sovereignty to cyberspace poses unique issues due to its borderless nature. Cyber activities often transcend traditional national boundaries, complicating efforts to

regulate and control them. Despite ongoing debates about states' ability to govern the global internet, attempts are made to apply traditional sovereignty principles to cyberspace.

Initially, we must address whether cyber sovereignty aligns with traditional sovereignty. This serves as our initial challenge.

3.1 Cyber Sovereignty in International Law

Sovereignty is fundamental in the current international system, signifying a state's authority within its territorial entity. Steven Krasner classifies sovereignty into four types: domestic, interdependence, international legal, and Westphalian sovereignty.

In the international system, cyber sovereignty encompasses a state's control over its cyber domain, including the internet, data, and information systems. It is an extension of traditional national sovereignty, reflecting a state's ability to safeguard its independence, control electronic systems, and protect national interests online.

Key aspects of cyber sovereignty include a state's right to determine internet policies, safeguard cyber networks, enforce cyber laws, protect sensitive data, and collaborate internationally on cyber issues. However, cyber sovereignty's application is complex, particularly in addressing cross-border cyber threats and attacks.

States have yet to formally acknowledge the independence of cyberspace. However, they impose territoriality in cyberspace by implementing control mechanisms over information flows. For instance, in the case of Yahoo!'s refusal to comply with France's request to cease auctioning Nazi-related items, a French court ruled that the company was subject to French law despite operating online.

Nevertheless, cyber sovereignty must have limits, as states are bound by international laws and human rights principles. International law recognizes that sovereignty principles apply to cyberspace. However, debates persist on whether sovereignty should be considered a fundamental rule or a guiding principle in international law.

Some states, like the United Kingdom, argue that sovereignty is a guiding principle rather than an independent rule in international law. Others, like the Netherlands and Finland, view sovereignty breaches as international wrongful acts.

Territoriality is crucial in embodying sovereignty, defining a state's territorial jurisdiction and its powers, interests, and identity. Therefore, efforts to subject cyberspace to national borders reflect the need to define cyber sovereignty and address issues in its application.

In conclusion, applying cyber sovereignty faces issues in reconciling borderless cyberspace with traditional territorial boundaries. While sovereignty principles apply to cyberspace, debates persist on its nature and application in international law. Efforts to regulate cyberspace reflect the ongoing evolution of sovereignty in the digital age.

3.2 Implementation Issues in National Law

Implementing cyber sovereignty in national law emphasizes states' rights to govern and regulate cyberspace within their borders. It encompasses establishing rules for internet activities, ensuring cybersecurity, and protecting national interests while acknowledging the global nature of the internet.

However, implementing cyber sovereignty presents several legal issues:

1. **Legal and Jurisdictional Authority**: The borderless nature of the internet complicates determining jurisdiction for online activities spanning multiple jurisdictions, leading to conflicts between legal systems and uncertainty over regulatory authority.
2. **Data Protection and Privacy**: Varying laws and regulations on data protection and privacy across countries create issues in ensuring consistent protection of individuals' data across borders.
3. **Freedom of Expression**: Balancing freedom of expression with the need to regulate harmful content online raises concerns about censorship and violations of the right to access information.
4. **Cybersecurity**: Ensuring cybersecurity within national borders and cooperating internationally to address cyber threats pose legal complexities, especially in identifying perpetrators and enforcing legal measures.
5. **Cross-Border Data Flow**: Legal issues arise regarding data localization requirements, cross-border data transfers, and protecting data privacy while facilitating the free flow of data necessary for businesses and services.

Addressing these legal issues requires international cooperation, stakeholder dialogue, and the development of regulatory frameworks.

4 Analysis of Legal Issues for Cyber Sovereignty

Since the Treaty of Westphalia in 1648, the modern nation-state model and the concept of national sovereignty have been upheld, as affirmed by the United Nations Charter. However, cyberspace poses a significant challenge to sovereignty, impacting states internally before affecting their societies.

Cyberspace influences states by facilitating the flow of data, information, goods, services, values, and cultures, potentially changing collective public opinion and inciting conflicts

between state institutions and society. This internal conflict weakens sovereignty, challenging the application of national law, judicial jurisdiction, security, privacy, and human rights.

States resist weakening sovereignty despite cyberspace's threat to national borders, as it enables unguided interaction between societies and manipulation of individual choices. Legal issues to cyber sovereignty affect economic, social, political, and security realms, often addressed with political and security tools rather than legal measures due to a lack of effective regulatory frameworks in international law.

To address these issues, we must revisit the concept of state sovereignty, rooted in community will and represented by the state to uphold human values, culture, and societal choices. Amidst the concepts of society, state, and cyber sovereignty, freedom and culture emerge as fundamental values shaping interactions in cyberspace. States strive to assert sovereignty over cyberspace to control information flow, overcoming the challenge of borders and defining boundaries in the digital realm.

5 Conclusion

In conclusion, cyber sovereignty represents an evolution in the concept of sovereignty, emerging from technological advancements and contemporary circumstances. While traditional sovereignty focuses on authority and control within geographic borders, cyber sovereignty emphasizes authority and control in cyberspace and the flow of data over the internet.

The application of cyber sovereignty in international and national law is crucial for addressing new issues posed by modern technology. It is an integral part of national sovereignty, affirming states' rights to regulate their cyberspace through laws and regulations. This enables states to maintain cybersecurity and protect national interests online. However, achieving this requires international cooperation and the development of an appropriate legal framework to ensure stability and security in the global cyberspace.

History illustrates how castle walls once protected civilizations by force, then national borders did so through law. However, the open cyberspace has transformed this dynamic, necessitating reliance on culture and awareness to protect sovereignty. Nations must build sovereignty through a culture of respect for the law, while states should work towards establishing effective international regulatory frameworks for cyberspace.

The legal issues of cyber sovereignty require a precise understanding of cyberspace dynamics and the development of suitable legal frameworks to balance national control and international cooperation.

References

Adams, J., Albakajai, M.: Cyberspace: a new threat to the sovereignty of the state, university of essex research repository. Manag. Stud. **4**(6), 256–265 (2016)

Al-Gharaibeh, S., Hijazi, H.A., Alzoubi, H.M., Abdalla, A.A., Khamash, L.S., Kalbouneh, N.Y.: The impact of e-learning on the feeling of job alienation among faculty members in Jordanian universities. ABAC J. **43**(4), 303–317 (2023)

Bellanger, P.: From sovereignty in general to digital sovereignty in particular. Les Echos.fr. **54**, 30 (2011)

Bu, F., Mahmoud, H.A., Alzoubi, H.M., Ramazanovna, N.K., Gao, Y.: Do financial inclusion, natural resources and urbanization affect the sustainable environment in emerging economies. Resour. Policy **87**, 104292 (2023)

Eli, T., Hamou, L.A.S.: Investigating the factors that influence students choice of English studies as a major: the case of university of Nouakchott Al Aasriya, Mauritania. Int. J. Technol., Innov. Manag. (IJTIM). **2**(1) (2022)

Foucault, M.: Power/Knowledge. In: Gordon, C. (ed.) Pantheon Books, New York (1980)

Guergov, S., Radwan, N.: Blockchain convergence: analysis of issues affecting IoT, AI and blockchain. Int. J. Comput., Inf. Manuf. (IJCIM) **1**(1)

von Heinegg, W.H.: Legal implications of territorial sovereignty in cyberspace. In: 4th international conference on cyber conflict. NATO CCD COE Publications, Tallinn (2012)

Hinsley, F.H.: The concept of sovereignty and the relations between states. J. Int. Aff. **21**(2), 242–252 (1967)

Ivanova, K., Myltykbaev, M., Shtodina, D.: The concept of cyberspace in international law. Law Enforc. Rev. (2022)

Krasner, S.D.: Sovereignty: Organized Hypocrisy. Princeton University Press, Princeton (1999)

Kuehl, D.T.: From cyberspace to cyberpower: defining the problem. Cyberpower Natl. Secur. **30** (2009)

Laguerre, M.: Virtual time, in information. Commun. & Soc. **7**(2), 223–247 (2004)

Mirza, M., Ali, L., Qaisrani, I., Mirza M.N., Ali, L.A., Qaisrani, I.H.: Webol. **18**(5) (2021)

Ong, A.: Powers of Sovereignty: State, people, wealth, life, Focaal (2012)

Renwick, A., Swinburn, I.: Upper secondary school valletta. Hyphen **7**(2), 67–78 (1992)

Schneider, G.: E-Business, 10th edn. Course Technology, Cengage Learning, London (2013)

Tsagouria, N.: Chapter 1: The legal status of cyberspace: sovereignty redux? Elgar online, 12 (2021)

Wu, T.S.: Cyberspace sovereignty? the internet and the international system. Harv. J. Law & Technol. **10**(3), 647–666 (1997)