Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

UDC 341.6 https://doi.org/10.33619/2414-2948/126/58

EVOLUTION OF THE CONCEPT OF "CYBER SOVEREIGNTY" IN INTERNATIONAL LAW

©**Chatak uulu A.,** *International University of Kyrgyzstan, г. Бишкек, Кыргызстан*

ЭВОЛЮЦИЯ КОНЦЕПЦИИ «КИБЕРСУВЕРЕНИТЕТА» В МЕЖДУНАРОДНОМ ПРАВЕ

©**Чатак уулу А.**, *Международный университет Кыргызстана, г. Бишкек, Кыргызстан*

Abstract. The article examines the evolution of the concept of "cyber sovereignty" within the framework of international law. As digital technologies reshape global governance and interstate relations, the traditional understanding of sovereignty is undergoing significant transformation in cyberspace. The study explores how states interpret and operationalize cyber sovereignty in response to transnational cyber threats, data governance challenges, and the increasing strategic importance of digital infrastructure. The research analyzes doctrinal approaches to cyber sovereignty, the applicability of classical principles of international law — such as territorial integrity, non-intervention, and due diligence — to cyberspace, and the growing tensions between national control over digital resources and the global nature of the Internet. Particular attention is paid to competing models of digital governance, including state-centric regulatory approaches and multistakeholder frameworks. The article also considers the implications of cyber sovereignty for human rights protection, cross-border data flows, and international cooperation in cybersecurity. Methodologically, the study employs formal-legal, comparative, and systemic analysis to assess the transformation of sovereignty in the digital age. The findings suggest that cyber sovereignty is evolving from a purely territorial notion toward a functional and regulatory paradigm that seeks to reconcile state authority with international legal obligations and the protection of fundamental rights. The article concludes that future international regulation must balance sovereign digital control with the need for interoperability, cooperation, and universal legal standards in cyberspace.

Аннотация. Рассматривается эволюция концепции «киберсуверенитета» в рамках международного права. Поскольку цифровые технологии меняют глобальное управление и межгосударственные отношения, традиционное понимание суверенитета претерпевает значительные изменения в киберпространстве. Исследование изучает, как государства интерпретируют и реализуют киберсуверенитет в ответ на транснациональные киберугрозы, проблемы управления данными и растущую стратегическую важность цифровой инфраструктуры. Анализируются доктринальные подходы к киберсуверенитету, применимость классических принципов международного права — таких как территориальная целостность, невмешательство и должная осмотрительность — к киберпространству, а также растущая напряженность между национальным контролем над цифровыми ресурсами и глобальным характером Интернета. Особое внимание уделяется конкурирующим моделям цифрового управления, включая государственно-центрированные регулятивные подходы и многосторонние структуры. В статье также рассматриваются последствия киберсуверенитета для защиты прав человека, трансграничных потоков данных и международного сотрудничества в области кибербезопасности. Методологически в исследовании используются формально-правовой, сравнительный и системный анализ для оценки трансформации суверенитета в цифровую эпоху. Результаты исследования показывают, что киберсуверенитет

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

эволюционирует от чисто территориального понятия к функциональной и регулятивной парадигме, стремящейся согласовать государственную власть с международно-правовыми обязательствами и защитой основных прав. В заключение статьи говорится, что будущее международное регулирование должно уравновешивать суверенный цифровой контроль с необходимостью совместимости, сотрудничества и универсальных правовых стандартов в киберпространстве.

Keywords: cyber sovereignty, international law, digital governance, state sovereignty, cyberspace regulation.

Ключевые слова: киберсуверенитет, международное право, цифровое управление, государственный суверенитет, регулирование киберпространства.

The rapid digitalization of social, economic, and political relations has fundamentally transformed the structure of international interactions and the understanding of state authority in the global arena. Cyberspace, once perceived as a borderless and decentralized environment, has increasingly become a domain of strategic competition, regulatory fragmentation, and normative contestation. In this context, the concept of cyber sovereignty has emerged as a central category in contemporary international legal discourse, reflecting states' efforts to assert authority over digital infrastructure, data flows, and information space within and beyond their territories.

Traditionally, sovereignty in international law has been grounded in territorial integrity, political independence, and the principle of non-intervention. However, the transnational architecture of the Internet challenges classical territorial assumptions and compels a re-evaluation of how sovereignty applies in cyberspace [2, 4]. Early narratives of a "borderless Internet" have gradually given way to more state-centric regulatory approaches, where governments seek to reassert control over digital networks, online platforms, and cross-border data exchanges [1, 3].

The debate on cyber sovereignty has intensified in parallel with the growing number of cyber incidents affecting critical infrastructure, electoral processes, and national security. Reports of the United Nations Group of Governmental Experts (UNGGE, 2015) and the Open-Ended Working Group (OEWG, 2021) affirm that existing principles of international law, including sovereignty and non-intervention, apply to cyberspace. Nevertheless, significant disagreement persists regarding the scope and operational meaning of these principles in the digital domain [7, 8]. The application of due diligence obligations, attribution standards, and state responsibility in cyber operations remains contested [5, 9]

At the same time, the notion of cyber sovereignty is not uniform. Competing models of digital governance illustrate divergent interpretations: some states advocate a strong sovereignty-based approach emphasizing national control over information flows and infrastructure, while others promote multistakeholder governance and interoperability of digital regimes [10]. These competing visions reflect broader geopolitical tensions and differing normative priorities, particularly regarding human rights, freedom of expression, and privacy in the digital sphere [12].

The evolution of cyber sovereignty thus raises fundamental theoretical and practical questions: How does the concept relate to classical doctrines of international law? Does cyber sovereignty represent a continuity of traditional territorial authority, or does it signal the emergence of a new functional and regulatory paradigm? How can sovereign digital control be reconciled with the global nature of the Internet and the need for international cooperation?

The purpose of this article is to examine the evolution of the concept of cyber sovereignty in international law and to assess its implications for global digital governance. The study aims to: 1)

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Analyze doctrinal interpretations of sovereignty in cyberspace; 2) Explore the development of UN-based normative frameworks; 3) Compare competing governance models; 4) Evaluate the prospects for harmonizing sovereign authority with international legal obligations.

Methodologically, the research relies on formal-legal analysis of international documents, comparative examination of regulatory approaches, and systemic analysis of the interaction between sovereignty, cybersecurity, and global governance. By situating cyber sovereignty within the broader evolution of international law, this article argues that the concept is undergoing a transition from a strictly territorial understanding toward a hybrid regulatory model that combines state authority with multilevel governance mechanisms and international normative constraints. In this evolving legal landscape, cyber sovereignty is not merely a political slogan but a dynamic doctrinal construct that will shape the future architecture of international law in the digital age.

This study employs a multidimensional methodological framework combining formal-legal, comparative, and systemic approaches to examine the evolution of the concept of cyber sovereignty in international law.

First, the formal-legal method is used to analyze primary sources of international law, including United Nations reports, state practice documents, and doctrinal interpretations of sovereignty in cyberspace. Particular attention is paid to the reports of the United Nations Group of Governmental Experts (UNGGE, 2015) and the United Nations Open-Ended Working Group (OEWG, 2021), which affirm the applicability of existing international law principles to cyberspace [7, 8]. The analysis also draws upon doctrinal interpretations presented in the *Tallinn Manual 2.0* [5], which provides an authoritative academic assessment of how sovereignty, non-intervention, and due diligence operate in cyber operations. Second, the comparative method is applied to examine different models of digital governance and interpretations of cyber sovereignty. The study contrasts state-centric regulatory approaches with multistakeholder governance frameworks [1, 4].

It also considers geopolitical dimensions and strategic competition in cyberspace as reflected in contemporary analyses of digital power and global cyber politics [12].

This comparative perspective allows for identifying divergent conceptualizations of cyber sovereignty across jurisdictions and governance traditions. Third, a systemic approach is employed to situate cyber sovereignty within the broader structure of international law and global governance. Rather than treating sovereignty as an isolated principle, the research analyzes its interaction with other core norms of international law, including territorial integrity, non-intervention, and state responsibility [9]. The study further considers how digital governance structures and Internet control mechanisms influence the transformation of sovereignty in practice [2, 9].

Additionally, elements of doctrinal analysis are incorporated to trace the conceptual evolution of sovereignty from classical territorial doctrine to its functional adaptation in cyberspace. By integrating normative documents, academic literature, and international practice, the research aims to provide a coherent theoretical explanation of how cyber sovereignty is emerging as a hybrid regulatory paradigm rather than a departure from traditional international law. This methodological combination ensures a comprehensive examination of both the normative foundations and the practical manifestations of cyber sovereignty in contemporary international law.

The conducted analysis demonstrates that the concept of cyber sovereignty has evolved from a narrow territorial extension of classical sovereignty toward a more complex regulatory and functional paradigm embedded in contemporary international law. The results reveal four major patterns in the doctrinal and practical development of cyber sovereignty.

One of the central findings of this study is the progressive consolidation of the principle that existing international law fully applies to cyberspace. Contrary to early assumptions that cyberspace might constitute a legally exceptional or “ungoverned” domain, contemporary international practice

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

demonstrates increasing agreement among states that digital activities fall within the scope of established international legal norms.

The reports of the United Nations Group of Governmental Experts (UNGGE, 2015) marked a decisive turning point by explicitly affirming that international law, and in particular the United Nations Charter, is applicable to state conduct in cyberspace. This recognition was subsequently reaffirmed and further elaborated in the report of the Open-Ended Working Group (OEWG, 2021), which emphasized that sovereignty, non-intervention, peaceful settlement of disputes, and state responsibility remain operative in the digital domain. These reports reflect not merely political consensus but an emerging opinio juris that cyberspace is not outside the normative reach of international law [7, 8].

The applicability of sovereignty in cyberspace has become a focal point of doctrinal debate. According to the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, sovereignty operates both as a principle and as a rule that may be violated by certain cyber operations that cause effects on another state's territory or interfere with inherently governmental functions [5]. The Manual clarifies that cyber operations resulting in physical damage, loss of functionality, or interference with critical infrastructure may constitute violations of sovereignty. This interpretation situates cyberspace firmly within the traditional legal architecture governing interstate relations.

Moreover, the principle of non-intervention has been interpreted as extending to coercive cyber activities directed at the domaine réservé of another state, including electoral processes, public administration systems, or critical infrastructure management [5]. The due diligence obligation — requiring states not to knowingly allow their territory to be used for acts that harm other states — has similarly been adapted to the digital context, implying that states must take reasonable measures to prevent malicious cyber activities emanating from infrastructure under their control [7, 8].

Importantly, this consolidation does not imply the creation of entirely new legal norms but rather the reinterpretation and functional adaptation of existing principles to technological realities. As emphasized in doctrinal literature, sovereignty in cyberspace is not displaced or replaced by a novel legal category; instead, it is operationalized through the lens of digital infrastructure, cross-border data flows, and remote cyber operations [5]. In this sense, cyber sovereignty emerges not as an autonomous doctrinal innovation but as a contextualized expression of classical sovereignty in a technologically mediated environment.

At the same time, the consolidation process remains incomplete. States diverge in their interpretation of what constitutes a breach of sovereignty in cyberspace, particularly regarding non-destructive cyber operations such as espionage, data exfiltration, or influence campaigns. While consensus exists regarding the applicability of international law in general terms, the precise thresholds for unlawful conduct continue to evolve through state practice and scholarly debate.

Nevertheless, the overall trajectory is clear: cyberspace is no longer perceived as a legal vacuum. The progressive reaffirmation of the applicability of international law, particularly through UN processes and authoritative doctrinal interpretations, demonstrates a structural normalization of cyberspace within the existing international legal order.

The study identifies a pronounced divergence in the interpretative models through which cyber sovereignty is conceptualized and operationalized in international legal and policy discourse. This divergence reflects not merely theoretical disagreement but fundamentally different visions of digital order, governance authority, and the role of the state in cyberspace.

The state-centric (regulatory sovereignty) model conceptualizes cyberspace as subject to comprehensive national jurisdiction analogous to territorial sovereignty. Under this approach, states assert regulatory authority over digital infrastructure, online platforms, and data flows within their territory and, in certain cases, beyond it. Central features of this model include data localization

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

requirements, strict content regulation, control over critical information infrastructure, and enhanced cybersecurity legislation.

Scholarly analysis of Internet governance has demonstrated how the early narrative of a borderless digital sphere gradually gave way to increasing state intervention and regulatory consolidation [4]. The growing securitization of cyberspace and geopolitical rivalry have further strengthened sovereignty-based approaches, as states seek to protect strategic digital assets and reduce technological dependence [12]. In this framework, cyber sovereignty is interpreted as an extension of traditional authority into digital space, emphasizing national resilience, autonomy, and strategic control.

In contrast, the multistakeholder or global governance model views cyberspace as a transnational domain requiring shared governance among states, private actors, technical communities, and civil society. Rather than emphasizing exclusive state control, this model promotes interoperability, openness, and distributed regulatory mechanisms. Internet governance institutions historically evolved through such multistakeholder processes, reflecting the technical and global nature of network architecture [[1].

The tension between these models stems from competing normative priorities. The state-centric model prioritizes national security, regulatory clarity, and political autonomy, whereas the multistakeholder model prioritizes innovation, global connectivity, and protection of digital rights. As geopolitical competition intensifies, particularly in areas such as cybersecurity, digital trade, and technological infrastructure, fragmentation pressures reinforce sovereignty-based interpretations [12].

Importantly, this divergence illustrates that cyber sovereignty is not a settled legal doctrine but a contested normative construct. Its meaning varies across jurisdictions and political systems, reflecting different balances between security, openness, and international cooperation. The absence of a universally accepted definition further confirms its dynamic and politically embedded nature.

Classical sovereignty in international law is territorially anchored: authority is exercised within clearly defined geographical boundaries, and jurisdiction corresponds to physical territory. However, cyberspace destabilizes this territorial logic. Digital networks transcend borders, data flows circulate globally, and cyber operations may be conducted remotely without physical presence. This structural transformation compels a reconceptualization of how sovereignty operates in practice.

The analysis demonstrates that sovereignty in cyberspace increasingly assumes a functional dimension, whereby authority is exercised not merely through territorial control but through regulatory capacity and governance mechanisms. Rather than focusing exclusively on physical borders, states assert sovereignty through the regulation of digital infrastructure, control over data processing activities, and oversight of online platforms.

Early critiques of the “borderless Internet” thesis already recognized that states would reassert regulatory authority in response to technological developments [2]. Contemporary doctrinal analyses further confirm that sovereignty in cyberspace functions through legal rules governing cyber operations, jurisdiction, and state responsibility [9]. This shift reflects a transformation from spatial sovereignty to regulatory sovereignty. This functional evolution manifests in several concrete areas:

1. Extraterritorial application of national cyber laws. States increasingly apply cybersecurity, data protection, or digital platform regulations beyond their territory, particularly when foreign entities process data of their citizens or affect national infrastructure;

2. Cross-border data regulation. Jurisdictional claims over data flows are asserted based on nationality, location of servers, or economic impact, rather than purely territorial presence;

3. Platform governance and content moderation.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

States regulate global digital platforms operating within their jurisdiction, requiring compliance with national content standards, cybersecurity obligations, and data governance rules.

These practices indicate that sovereignty is becoming operationalized through regulatory reach and technological leverage, rather than territorial exclusivity alone. Authority is exercised via licensing regimes, compliance mechanisms, digital infrastructure standards, and technical controls.

However, this functional transformation also generates legal complexity. Overlapping regulatory claims may produce jurisdictional conflicts and contribute to the fragmentation of the global digital space. The functionalization of sovereignty thus strengthens regulatory capacity while simultaneously increasing the risk of normative collisions between national regimes.

The findings of this study demonstrate that cyber sovereignty cannot be conceptualized solely as an expression of state authority over digital infrastructure and information space. Rather, it operates within a normative framework structured by international human rights law. In contemporary international legal discourse, sovereignty in cyberspace is increasingly conditioned by obligations arising from universal and regional human rights instruments.

Expansive interpretations of sovereign digital control — such as mandatory data localization, extensive content regulation, or large-scale digital surveillance — may directly affect freedom of expression, access to information, and the right to privacy. Research highlights that state-driven regulation of digital space often reflects security-driven rationales but may simultaneously narrow civic space and restrict online freedoms [3]. Similarly, critical analyses of digital sovereignty discourse reveal that the language of sovereignty can be instrumentalized to legitimize centralized control over information ecosystems [10].

At the same time, international processes within the United Nations framework increasingly integrate human rights considerations into discussions of responsible state behavior in cyberspace. The UNGGE (2015) explicitly affirmed that international law, including human rights law, applies to state conduct in cyberspace. This position was reinforced by the OEWG (2021), which emphasized that states must ensure that measures to enhance cybersecurity are consistent with their obligations under international human rights law. These reports signal an important normative development: cyber sovereignty is not absolute but embedded within a hierarchy of international legal commitments [7, 8].

This interdependence produces a structural duality. On the one hand, sovereignty legitimizes state action to protect national security and public order in the digital domain. On the other hand, human rights norms act as limiting principles that prevent disproportionate or arbitrary interference. The principle of proportionality, procedural safeguards, and judicial oversight function as mechanisms that reconcile security objectives with rights protection. Moreover, digital governance increasingly reflects a shift from unilateral sovereignty claims toward internationally accountable sovereignty. States asserting regulatory authority over cyberspace are simultaneously subject to scrutiny regarding the human rights implications of such measures. This normative constraint contributes to the transformation of cyber sovereignty from a purely power-based concept into a legally conditioned authority.

The findings of this study indicate that the evolution of cyber sovereignty reflects a broader structural transformation of international law in response to technological change. Rather than displacing classical sovereignty, cyberspace has become a domain in which traditional principles are reinterpreted, contested, and operationalized through new regulatory mechanisms. This discussion situates the results within contemporary doctrinal debates and evaluates their broader normative implications.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Table 1

EVOLUTIONARY STAGES OF CYBER SOVEREIGNTY IN INTERNATIONAL LAW

Stage	*Core Characteristics*	*Dominant Logic*	*Normative Implication*
Early Internet Era	Cyberspace perceived as borderless and decentralized	Minimal territorial control	Weak state intervention
Institutional Recognition	Formal affirmation of applicability of international law	Continuity of sovereignty	Cyberspace integrated into existing legal order
Geopolitical Assertion	Emphasis on digital autonomy, data control, strategic competition	Regulatory sovereignty	Fragmentation and securitization
Functional Adaptation	Integration of sovereignty with global governance mechanisms	Regulatory-functional sovereignty	Hybrid, conditional sovereignty
Human Rights Conditioning	Sovereignty constrained by human rights obligations	Legally conditioned sovereignty	Rights-based limitation of digital authority

Table 2

COMPETING MODELS OF CYBER SOVEREIGNTY

Model	*Key Features*	*Strengths*	*Risks*	*Human Rights Dimension*
State-Centric Model	Data localization; infrastructure control; strong jurisdictional claims	National security enhancement; policy coherence	Internet fragmentation; reduced cross-border interoperability	Higher risk of disproportionate restrictions
Multistakeholder Model	Distributed governance; private sector participation; global coordination	Innovation; flexibility; global connectivity	Limited state enforcement capacity; regulatory gaps	Stronger protection of openness and expression
Hybrid Model	Sovereign authority combined with international standards and oversight	Balanced regulatory capacity; adaptive governance	Normative ambiguity; implementation complexity	Conditional sovereignty under human rights constraints

First, the consolidation of the applicability of international law to cyberspace confirms a strong continuity thesis. The affirmation by the United Nations Group of Governmental Experts (UNGGE, 2015) and the Open-Ended Working Group (OEWG, 2021) that the UN Charter and existing international law apply to cyberspace reinforces the view that digital space does not constitute a legal vacuum [7, 8]. This position aligns with doctrinal interpretations presented in *Tallinn Manual 2.0*, which emphasize that sovereignty, non-intervention, and due diligence remain foundational principles governing cyber operations [5]. However, while applicability is widely accepted, the thresholds for violations of sovereignty remain disputed, particularly in cases of non-destructive cyber operations. This ambiguity suggests that cyber sovereignty is still in a phase of interpretative development rather than doctrinal stabilization.

Second, the divergence between state-centric and multistakeholder governance models highlights the political dimension of cyber sovereignty. As Mueller (2010) and DeNardis (2014) demonstrate, Internet governance historically evolved through decentralized and multistakeholder arrangements [[1, 4]. Yet, geopolitical competition and security concerns have encouraged states to reassert centralized regulatory authority [12]. This tension produces a fragmented normative

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

environment in which sovereignty is interpreted differently depending on strategic interests and governance philosophies. The discussion therefore confirms that cyber sovereignty is not a neutral legal concept but a politically embedded construct shaped by competing visions of digital order.

Third, the shift from territorial to functional sovereignty reflects the technological realities of cyberspace. Goldsmith and Wu (2006) anticipated that states would reassert control over digital networks despite early narratives of borderlessness [2].

Contemporary practice confirms this prediction: regulatory authority is increasingly exercised through control of infrastructure, data governance regimes, and platform compliance mechanisms. Tsagourias and Buchan (2015) argue that the application of sovereignty to cyberspace requires contextual interpretation rather than formal territorial analogies. This supports the conclusion that sovereignty is evolving into a capacity-based concept grounded in regulatory power rather than geographic exclusivity [9].

Fourth, the interdependence between cyber sovereignty and human rights significantly shapes the contemporary debate. While sovereignty legitimizes digital regulation, human rights norms impose substantive and procedural constraints. MacKinnon (2012) warns that expansive digital control may erode freedom of expression and online autonomy. Similarly, Couture and Toupin (2019) demonstrate that sovereignty discourse can serve as a justificatory framework for centralization of information control [3, 10].

The UN processes explicitly recognize that state behavior in cyberspace must comply with international human rights obligations. This suggests that cyber sovereignty is increasingly conditioned by normative limits, reinforcing its embeddedness within the broader international legal order. The discussion also reveals an emerging paradox: while states seek greater sovereign control over digital space to enhance security and autonomy, excessive unilateralism risks fragmentation of the global Internet and normative inconsistency. The functional expansion of sovereignty strengthens national regulatory capacity but may undermine interoperability and cooperative cybersecurity mechanisms. As DeNardis (2014) notes, digital governance is inherently transnational; therefore, unilateral sovereignty claims must coexist with collaborative frameworks [1].

In sum, the evolution of cyber sovereignty reflects a process of legal adaptation rather than rupture. The concept operates at the intersection of continuity (application of existing international law), transformation (functionalization of sovereignty), and contestation (divergent governance models). Its future trajectory will likely depend on the balance between geopolitical competition and institutionalized cooperation within multilateral frameworks. These findings contribute to the theoretical debate by clarifying that cyber sovereignty should be understood not as an autonomous doctrinal innovation but as a dynamic interpretative layer within international law. The discussion underscores that sovereignty in cyberspace remains legally bounded, politically negotiated, and technologically conditioned. The evolution of the concept of cyber sovereignty reflects a broader transformation of international law under the pressures of digitalization and technological interdependence. The study demonstrates that cyber sovereignty does not constitute a radical departure from classical doctrines of sovereignty but rather represents their contextual adaptation to the realities of cyberspace. International law, including the principles of sovereignty, non-intervention, due diligence, and state responsibility, remains fully applicable in the digital domain, as affirmed in UN processes and doctrinal analyses [5].

At the same time, the interpretation of sovereignty in cyberspace is neither uniform nor settled. The divergence between state-centric and multistakeholder governance models illustrates that cyber sovereignty functions as a contested normative construct shaped by geopolitical, technological, and regulatory considerations [1, 4, 12].

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

The growing securitization of cyberspace has reinforced sovereignty-based regulatory approaches, yet digital interdependence simultaneously necessitates cooperative governance mechanisms. A key finding of this research is the functional transformation of sovereignty. Rather than being confined to territorial control, sovereignty increasingly operates through regulatory capacity—via infrastructure governance, cross-border data regulation, and oversight of digital platforms [2, 9]. This shift signals the emergence of a regulatory-functional model of sovereignty in cyberspace, grounded not in physical borders but in normative and institutional authority. Equally significant is the recognition that cyber sovereignty is structurally conditioned by international human rights law. Sovereign digital authority is not absolute; it must be exercised consistently with obligations concerning freedom of expression, privacy, and procedural safeguards [3, 11].

UN frameworks explicitly reaffirm that responsible state behavior in cyberspace must comply with international legal and human rights standards [7, 8].

Thus, sovereignty in the digital era operates within a system of normative constraints that prevent its transformation into unrestricted control. In theoretical terms, cyber sovereignty should be understood as a dynamic and evolving doctrinal construct that integrates continuity and transformation. It reflects the enduring relevance of state authority while simultaneously adapting to the transnational and technologically mediated nature of cyberspace. Future developments in international law will likely determine whether cyber sovereignty consolidates as a harmonized regulatory paradigm or remains fragmented across competing governance models. Its trajectory will depend on the ability of states and international institutions to reconcile sovereign authority with cooperation, interoperability, and respect for fundamental rights. Ultimately, the evolution of cyber sovereignty demonstrates that international law is not rendered obsolete by digital transformation; rather, it evolves through interpretative adaptation, institutional practice, and normative negotiation.

References:

1. DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

2. Goldsmith, J. (2007). Who controls the Internet? Illusions of a borderless world. *Strategic Direction*, *23*(11). https://doi.org/10.1108/sd.2007.05623kae.001

3. MacKinnon, R. (2012). Consent of the networked: The worldwide struggle for Internet freedom. *Politique étrangère*, *50*(2), 432-463.

4. Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. MIT press.

5. Schmitt, M. N. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

6. Segura-Serrano, A. (2006). Internet regulation and the role of international law. *Max Planck Yearbook of United Nations Law Online*, *10*(1), 191-272.

7. United Nations Group of Governmental Experts (UNGGE). (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations.

8. United Nations Open-Ended Working Group (OEWG). (2021). *Final substantive report on developments in the field of ICTs in the context of international security*. United Nations.

9. Tsagourias, N., & Buchan, R. (2015). *Research handbook on international law and cyberspace*. Edward Elgar Publishing.

10. Couture, S., & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322.

11. Jiang, M. (2018). The business and politics of search engines: A comparative study of Baidu and Google. *Global Media and Communication*, 14(3), 283–299.

12. Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs.

Список литературы:

1. DeNardis L. The global war for internet governance. Yale University Press, 2014.
2. Goldsmith J. Who controls the Internet? Illusions of a borderless world // Strategic Direction. 2007. V. 23. №11. https://doi.org/10.1108/sd.2007.05623kae.001
3. MacKinnon R. Consent of the networked: The worldwide struggle for Internet freedom // Politique étrangère. 2012. V. 50. №2. P. 432-463.
4. Mueller M. L. Networks and states: The global politics of Internet governance. – MIT press, 2010.
5. Schmitt M. N. Tallinn manual 2.0 on the international law applicable to cyber operations. – Cambridge University Press, 2017.
6. Segura-Serrano A. Internet regulation and the role of international law // Max Planck Yearbook of United Nations Law Online. 2006. V. 10. №1. P. 191-272.
7. United Nations Group of Governmental Experts (UNGGE). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations. 2015.
8. United Nations Open-Ended Working Group (OEWG). Final substantive report on developments in the field of ICTs in the context of international security. United Nations. 2021.
9. Tsagourias N., Buchan R. Research handbook on international law and cyberspace. Edward Elgar Publishing. 2015.
10. Couture S., Toupin S. What does the notion of “sovereignty” mean when referring to the digital? // New Media & Society. 2019. V. 21. №10. P. 2305–2322.
11. Jiang M. The business and politics of search engines: A comparative study of Baidu and Google // Global Media and Communication. 2018. V. 14. №3. P. 283–299.
12. Segal A. The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. PublicAffairs. 2016.

Поступила в редакцию
06.03.2026 г.

Принята к публикации
15.03.2026 г.

Ссылка для цитирования:

Chatak uulu A. Evolution of the Concept of “Cyber Sovereignty” in International Law // Бюллетень науки и практики. 2026. Т. 12. №5. С. 472-481. https://doi.org/10.33619/2414-2948/126/58

Cite as (APA):

Chatak uulu, A. (2026). Evolution of the Concept of “Cyber Sovereignty” in International Law. *Bulletin of Science and Practice, 12*(5), 472-481. https://doi.org/10.33619/2414-2948/126/58