The Transformation of State Sovereignty in the Digital Age: Theoretical and Practical Challenges of Cyber Sovereignty

Banovsha Abbasova[1], Tabriz Jafarov[2]
[1,2]ADA University, Baku, Azerbaijan
[1]*babbasova20398@ada.edu.az*, [2]*tjafarov@ada.edu.az*

***Abstract*— This paper examines cyber sovereignty as a challenge to traditional conceptions of state sovereignty grounded in territorial authority. It argues that cyber sovereignty should be understood as a dynamic and hybrid concept shaped by legal norms, technological architecture, and institutional practices. The analysis addresses key practical problems, including transboundary jurisdiction, attribution of cyber operations, and tensions between security measures and rights, with particular reference to Yahoo v. France. It further evaluates national and international responses, concluding that existing frameworks enhance coordination but remain constrained by structural features of cyberspace.**

Keywords*— *cyber sovereignty; cyberspace governance; transboundary jurisdiction; attribution of cyber operations; international law; cybersecurity strategies; state responsibility; digital regulation.

I. INTRODUCTİON

Digital technologies have significantly influenced not only how human beings interact with each other, but also the manner in which power is exercised. The understanding of cyberspace has emerged as the core of all economic activities, all political processes, all security measures, and all social processes. The manner in which states can effectively govern their citizens is therefore inextricably linked to how they deal with activities that happen outside their borders but have a real impact inside their borders. This phenomenon has brought the notion of sovereignty into direct conflict with the technical aspects of the Internet.

Unlike other spheres in which public international law applies, cyberspace does not have geographical boundaries that can be linked with the notion of state sovereignty. The phenomenon of cyberspace is therefore characterized by a lack of connection between the location of the infrastructure, users, service providers, and the location of the activity. This leads to a lack of clarity not just with respect to the limits of state authority, but also with respect to the legality of intervention.

The situation is further complicated by the fact that in cyberspace, authority is exercised not only by states. Rather, there are a variety of actors, including private actors, who exercise authority over platforms, networks, and standards. These actors have assumed roles traditionally performed by public authorities in regulating the behavior of actors in cyberspace. The situation thus indicates a challenge to the traditional view of authority as necessarily centralized in sovereign states.

The international legal system also seems to struggle with dealing with issues in cyberspace. There is general agreement that international law applies to activities in cyberspace as well. However, there is uncertainty on how the basic principles of international law, such as sovereignty, jurisdiction, and non-intervention, apply to cyberspace. The lack of clarity in international law with regard to cyberspace is further supported by differences in practices. The content, scope, and implications of cyber sovereignty are, however, not clear. The paper addresses these issues in the context of the theoretical and practical problems in the exercise of state sovereignty in cyberspace. It thus treats the issue of cyber sovereignty not as a static phenomenon, but rather as a dynamic and evolving concept.

II. CHALLENGES TO TRADİTİONAL STATE SOVEREİGNTY İN CYBERSPACE

The rapid digitalization of social, economic, and political life has transformed the environment in which state sovereignty functions. Traditional sovereignty was based on territorial control and exclusive authority within physical borders, but cyberspace goes beyond geographic limits. The global structure of the Internet challenges traditional ideas of jurisdiction, law enforcement, and non-interference. For a long time, cyberspace was seen as a "borderless" space beyond the reach of state authority. Even some internet pioneers claimed that after the hegemony of the code, states will not be able to regulate the actions of humans on cyberspace [1]. In fact, their true ambition was to undermine the classical concept of sovereignty. However, this view has been critically reconsidered. In "Who Controls the Internet?", Goldsmith and Wu argue that the notion of a completely ungovernable Internet is misleading; states still retain significant power to regulate online activity through domestic laws, technical measures, and economic influence.

In his response to authors who argue for the uncontrollability of the Internet, if internet wants to be controlled, such control can also be exercised through its intermediaries. For instance, the people using the Internet, the Internet service providers offering access, and other similar intermediaries have a physical presence. Consequently, each

DOI: 10.25045/cyber.gov.2026.26

country employs extensive technological and other infrastructure to provide Internet access, which is located within the respective state’s territory. Therefore, to claim that cyberspace is uncontrollable from a national perspective while abstracting all these physical infrastructures from their social components is simply unreasonable [2].

History suggests that Goldsmith and his supporters may have been right in arguing that states would ultimately reassert their authority over global internet companies. Over time, many major technology firms have accepted the primacy of national legal systems and complied with domestic regulations.

For example, in the Yahoo! France case, French courts required Yahoo! to prevent French users from accessing Nazi memorabilia auctions hosted on its U.S.-based platform. Ultimately, Yahoo! complied with the ruling, effectively recognizing the applicability of French law to its services accessible within France.

Similarly, Meta Platforms (formerly Facebook) has complied with national legal requirements in several jurisdictions, including France and Germany, by removing unlawful content, adjusting data practices, and adhering to local court decisions. These actions reflect an acknowledgment that domestic legal systems can assert jurisdiction over global digital platforms when their services operate within national territories.

At the same time, the governance of the Internet highlights that digital infrastructure itself is placed within political power dynamics. Milton Mueller demonstrates that control over critical resources, such as the root of the Domain Name System (DNS), is not merely a technical matter but a deeply political one, involving states, private actors, and international institutions. This complexity shows that cyberspace is far from a neutral global commons; rather, it is a controversial regulatory space [3].

Moreover, as Lawrence Lessig observed, the architecture of cyberspace shapes behavior in ways comparable to legal norms. This insight is essential for understanding modern sovereignty. In cyberspace, control is exercised not only through legislation but also through technological design—through filtering systems, data localization requirements, encryption standards, and platform governance structures. Consequently, sovereignty increasingly operates through technological and infrastructural control, rather than being limited to territorial enforcement [4].

However, this does not mean that cyberspace can be described as an unregulatable space for states, or that states lack the tools and leverage necessary for its regulation.

The urgency of this issue is further emphasized by the rising number of cyber operations targeting critical infrastructure, electoral processes, and national security systems. These developments have raised debates within international law. The Tallinn Manual 2.0 affirms that sovereignty extends to cyberspace, yet disagreements still exist regarding the precise threshold at which cyber operations regulate violations of sovereignty or unlawful intervention. [5] Similarly, the UN Group of Governmental Experts (UN GGE) recognizes that existing international law applies to cyberspace but has not resolved various interpretations concerning state responsibility and attribution [6].

On the contrary, in “In Search of Jefferson’s Moose”, David G. Post offers a strong criticism of state-centered sovereignty in cyberspace by highlighting the potential for autonomous digital lawmaking communities. He suggests that law has a self-fulfilling character: its authority rests on the collective belief in its legitimacy. In this sense, online communities are capable of creating “real law” when participants recognize and accept it as binding. This perspective challenges the traditional assumption that only territorially grounded sovereigns are capable of producing a valid legal order. At the same time, Post acknowledges that conventional state law continues to shape and constrain behavior online. Yet he poses a fundamental jurisdictional question: “Which law? Whose law?”. Because the international legal system is built upon mutually recognized physical borders between sovereign states, the borderless flow of information across digital networks creates serious challenges for applying territorially based authority to online activity.

Post further demonstrates the functional autonomy of governance in cyberspace through the example of the UDRP, which resolves thousands of domain name disputes without relying on state enforcement. Although it lacks traditional sovereign backing, the UDRP “operates directly on the thing itself” and exercises effective governance within the digital namespace. Taken together, these arguments support the view that cyberspace can sustain legal orders structurally independent of state sovereignty [7].

Consequently, the relevance of state cyber sovereignty lies in the tension between two realities: the globally interconnected, technical nature of the Internet, and the insistent, territorially based structure of the international legal system. This tension creates deep theoretical and practical challenges, covering jurisdiction, enforcement, accountability, and the slim balance between security and fundamental rights.

III. Practical Challenges to the Exercise of State Authority in Cyberspace: Yahoo! Inc. v. France case

Application of national law to foreign-based platforms is one of the most persistent practical challenges to states' authority in cyberspace. Traditional jurisdictional doctrines are grounded in territorial presence; however, online activities frequently involve actors, infrastructure, and data located across multiple jurisdictions. This structural diversity complicates enforcement and raises concerns about extraterritorial competence.

The landmark Yahoo! Inc. v. France case illustrates this difficulty. Yahoo! Inc. v. France represents one of the earliest and most influential judicial confrontations between territorial sovereignty and the global architecture of the Internet. The case occurred when French anti-racism organizations initiated proceedings against Yahoo! Inc., a U.S.-based Internet service provider, for hosting auctions of Nazi memorabilia on its platform. Such content was lawful under U.S. law and hosted on servers located outside France. Still, it was accessible to users within French territory, where the display and sale of Nazi symbols are criminally prohibited.

In its order of 22 May 2000, the Tribunal de grande instance de Paris claimed jurisdiction over Yahoo on the basis that the harmful effects of the online activity were felt within France. The court rejected the argument that the extraterritorial location of servers excluded jurisdiction, although the content was accessible to French users. The French court affirmed its jurisdiction and upheld the applicability of national law to a foreign Internet platform based on territorial effects. This case resulted in a complex jurisdictional stalemate where the French order stood in France, but was held unenforceable in the US [8].

The Yahoo decision is significant because it demonstrates how states seek to claim sovereign authority in cyberspace by targeting intermediaries rather than attempting to regulate the Internet as a whole. As Goldsmith and Wu observe, the case emphasizes a broader strategy through which states regulate global networks by imposing obligations on entities with sufficient economic or operational ties to their jurisdiction. From this perspective, Yahoo illustrates not the impossibility of Internet regulation, but the adaptability of sovereign power in the digital environment [2].

At the same time, the case exposes the structural limits of such regulatory strategies. Following the French decision, Yahoo initiated proceedings in the United States seeking a declaration that the French order was unenforceable on First Amendment grounds. The case thus illustrates how transboundary Internet regulation can lead to normative clashes between states, particularly where freedom of expression, public order, and historical memory are regulated differently across jurisdictions.

Legal scholars have emphasized that Yahoo raises questions about legal certainty in cyberspace. Perritt notes that the case reflects a broader judicial tendency without clear limiting principles; therefore, this unclearity increase unpredictability for global service providers [9]. Similarly, de Hert, Parlar, and Thumfart analyize Yahoo case by emphasizing that courts justify cross-border assertions of authority through functional or effects-based reasoning, while leaving unresolved the risk of overlapping and conflicting legal obligations [10].

From the perspective of cyber sovereignty, Yahoo v. France occupies an uncertain position. It supports the claim that states are neither powerless nor irrelevant in cyberspace; territorial law can still shape online behavior through targeted enforcement and intermediary regulation. On the other hand, the case reveals the absence of a clear and consistent international framework capable of reconciling competing jurisdictional claims and addressing enforcement difficulties. Rather than resolving the tension between territorial sovereignty and global networks, the Yahoo case demonstrates that this tension constitutes a persistent structural feature of cyberspace governance.

The second significant practical challenge is related to the issue of attribution of cyber operations and, consequently, the issue of state responsibility. In contrast to conventional attacks or territory violations, cyber operations may be carried out anonymously, with the use of various routes passing through different countries’ territories, as well as by using civilian infrastructure. In this regard, it is difficult to establish who is responsible for the cyber operation.

The Tallinn Manual 2.0 states that a state bears responsibility for cyber operations attributable to it under the international law of state responsibility; however, there are substantial evidentiary and technical challenges in making attribution (Tallinn Manual 2.0, Rules 6-8 and 15, commentary pp. 80-88) [5]. These challenges are not merely theoretical. According to "Is International Law of Cyber Security in Crisis?" by Kubo Mačák, the lack of clarity on attribution has contributed to the overall instability of the international legal framework on cybersecurity and has raised questions about the effectiveness of current norms. States tend to use intelligence assessments and political attribution, rather than judicial standards of proof, and thereby increasingly weaken the role of law in regulating cyber conduct [11]. Goldsmith makes a similar point about the enforcement of cyber sovereignty in cyberspace, which may depend less on legal mechanisms than on power, leverage, and the regulation of local intermediaries, especially in cross-border cases. Attribution is therefore one of the most important obstacles to the effective exercise of cyber sovereignty [12].

VI. NATİONAL AND INTERNATİONAL APPROACHES TO ENSURİNG CYBER SOVEREİGNTY

At the national level, one of the most important tools for the protection of cyber sovereignty is the development of cybersecurity strategies. These strategies allow countries to systematically identify cyber threats, prioritize sectors, and assign responsibilities among relevant authorities. In this respect, the Final Report of the UN Open-Ended Working Group clearly encourages states to formulate and regularly update their national cybersecurity strategies as a tool for enhancing overall national resilience and improving response mechanisms against cyber threats [13].

Azerbaijan has taken this approach by formulating the Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023-2027, which clearly identifies cybersecurity as a vital part of national security. The strategy highlights the need for inter-institutional coordination, capacity-building, and the development of state capabilities in the cyber world. In this respect, special focus is given to the protection of critical information infrastructure, which is a key aspect of cyber sovereignty. On the other hand, by a decree of the Cabinet of Ministers, Azerbaijan formally defined critical information infrastructure and established a framework for its cybersecurity protection [14].

Pursuant to this decision, the National Cybersecurity Center was created as the competent authority responsible for ensuring the cybersecurity of critical infrastructure. The Center is tasked with coordinating protection measures, monitoring cyber threats, and overseeing compliance with national cybersecurity requirements in sectors designated as critical. At the same time, the Cabinet of Ministers of Azerbaijan has approved the official list of critical information infrastructure entities. This list is classified and not publicly disclosed, due to national security considerations [15].

International and regional documents increasingly require states to impose security and risk management obligations on the operators of essential services, particularly in sectors such as energy, transport, banking, and healthcare. The EU NIS Directive takes this approach by requiring Member States to ensure that operators of essential services apply appropriate technical and organizational measures to manage cyber risks [16]. Similarly, the national strategy of Azerbaijan has identified critical infrastructure as a priority area and seeks to enhance technical and regulatory mechanisms aimed at protecting the infrastructure from cyber threats [17].

Effective cyber sovereignty at the national level also depends on the adaptation of domestic legal frameworks to digital realities. In this respect, the Budapest Convention on Cybercrime establishes minimum substantive and procedural standards for national legislation, including the criminalization of cyber offences and the provision of investigative and evidentiary powers necessary to address cybercrime [18]. As a Party to the Convention, Azerbaijan has undertaken obligations to align its domestic criminal and procedural law with these standards, thereby reinforcing its legal capacity to respond to cybercrime and to cooperate in cross-border cyber investigations

At the international level, the exercise of cyber sovereignty is inextricably linked to cooperation between states. The 2015 Report of the UN Group of Governmental Experts highlights the need for international cooperation, information sharing, and mutual assistance in responding to cyber incidents and mitigating their effect [19]. In this regard, international efforts have been dedicated to the development of a set of shared norms of responsible state behavior in cyberspace. The UN OEWG Final Report confirms that international law applies in cyberspace and explicitly reaffirms the relevance of principles such as sovereignty, non-intervention, and state responsibility, thus providing a common normative framework for state behavior [13].

Apart from the global processes, regional legal systems also have an important role in dealing with the cross-border jurisdictional problems. In the European Union, for instance, there are legal instruments such as the European Investigation Order and the initiatives on electronic evidence that aim to standardize the access to the data stored beyond borders using legal procedures [20]. These examples show that the cross-border jurisdictional problems in cyberspace can be dealt with by using regional mechanisms.

Although these national and international efforts represent an increasing institutional focus on cyber sovereignty, their effectiveness is still complicated. International assessments have shown that the development and implementation of cybersecurity strategies and legal frameworks have led to an improvement in the states' ability to coordinate, prepare, and respond to incidents. For example, the UN OEWG Final Report states that national strategies are "an important step towards improved resilience and awareness," but also states that there are still "capacity challenges" and "implementation gaps" in the states' ability to implement these strategies, particularly in developing and transition economies [13].

At the national level, strategies such as Azerbaijan's Information Security and Cybersecurity Strategy offer an institutional framework for dealing with cyber threats, although their success is ultimately dependent on their implementation and effectiveness. International experience suggests that having these strategic documents on paper does not necessarily mean that cybersecurity will follow, particularly if the institutional coordination, technical expertise, or resources are not available. Indeed, international experience suggests that the presence of strategic documents does not necessarily lead to cybersecurity, particularly if the institutional coordination, technical expertise, or resources are not available. This is also reflected in regional practice under the NIS Directive, where the degree of implementation of the Directive has led to varying levels of protection for Member States, despite their shared legal obligations [16].

At the international level, cooperation and normative frameworks have led to increased attention on key principles, including the application of international law to cyberspace and the need for responsible state behavior. However, existing reports also acknowledge that these frameworks have not addressed the underlying challenges of attribution, enforcement, and jurisdiction. As such, while these strategies and frameworks represent a step forward in institutional focus on cyber sovereignty, they have not addressed the underlying tensions in cyberspace governance. Instead, they represent a tool that helps to mitigate risks and improve coordination, but have not addressed the underlying limitations imposed by the decentralized and border-transcending nature of cyberspace.

CONCLUSİON

As made clear in the analysis, the concept of cyber sovereignty cannot be reduced to a mere extension of the traditional territorial sovereignty of states into the cyber domain. Although states remain active in asserting their sovereignty over cyberspace, the structural properties of the Internet, such as its transboundary nature, dependence on private actors, and technological architecture, significantly alter the manner in which sovereign power is exercised. Throughout the course of this research, the concept of cyber sovereignty is not in decline but is instead undergoing a transformation, which relies on a variety of legal, technical, institutional, and international mechanisms.

Challenges such as transboundary jurisdiction, attribution of cyber attacks, and the relationship between security needs all made clear the continued disparity between legal theory and technological reality. Instances such as the Yahoo v. France case have made clear the malleability of state sovereignty as well as the lack of any comprehensive international framework that can effectively mediate competing claims of jurisdiction.

Concurrently, the examination of the national and international responses indicates that there has been significant progress. National cybersecurity policies, the protection of critical infrastructure, and the establishment of legal frameworks that are consistent with international norms have enhanced state capacity and cooperation. International and regional frameworks, especially in the United Nations and

regional bodies, have facilitated greater normative convergence and cooperation.

From a scientific point of view, this research makes a contribution to the understanding of cyber sovereignty as a dynamic and hybrid notion that cannot be reduced to either territorial control or technological determinism. From a practical standpoint, this research indicates that cyber sovereignty can be most effectively realized not as a matter of absolute domination but through a measured legal and institutional response that seeks to balance security, cooperation, and the safeguarding of rights.

In conclusion, cyber sovereignty must be considered as a process in and of itself, rather than a fixed legal condition. As the nature of cyberspace continues to evolve, states must correspondingly adapt their legal and policy frameworks to reflect both the potential and the limitations of sovereign power in a globally networked digital space.

REFERENCES

[1] P. Barlow, "A Declaration of the Independence of Cyberspace, 18 Duke Law & Technology Review 5-7 (2019)".

[2] J. L. Goldsmith A. Tim Wu, Who Controls The Internet? Lllusions Of Borderless World, New York: Oxford Unıversity Press, 2006.

[3] M. L. Mueller, Ruling the Root: Internet Governance and the Taming of Cyberspace, London: The MİT Press, 2002.

[4] L. Lessig, Code and Other Laws of Cyberspace, New York: Basic Books, 1999.

[5] Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations Prepared By The International Groups Of Experts At The Invitation Of The Nato Cooperative Cyber Defence Centre Of Excellence (General Editor Michael N. Schmitt, Managing Editor Lıı, Cambridge University Press, 2017.

[6] UN Group of Governmental Experts, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN Doc A/70/174, 2015).

[7] D. G. Post, In Search of Jefferson’s Moose: Notes on the State of Cyberspace., Oxford: Oxford University Press, 2009.

[8] LICRA and UEJF v Yahoo! Inc and Yahoo France, Tribunal de grande instance de Paris, Interim Order of 22 May 2000.

[9] H. P. Jr, ‘Jurisdiction in Cyberspace’, 41 Vill. L. Rev. 1 , 1996.

[10] C. P. a. J. T. Paul de Hert, "Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland," New Journal of European Criminal Law, pp. 1-27, 2018.

[11] K. Mačák, "Is the International Law of Cyber Security in Crisis?," in Cyber Power, N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.) 2016 © NATO CCD COE Publications, Tallinn, 2016, pp. 127-139.

[12] L. Goldsmith, "The Internet and the Abiding Significance of Territorial Sovereignty," Indiana Journal of Global Legal Studies, no. Vol. 5: Iss. 2, Article 6, pp. 475-491, 1998.

[13] "UN Open-Ended Working Group, Final Report (UN Doc A/75/816, 2021), paras. 34–36, 41.".

[14] "Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları”, July 17, 2023, as Decision No. 229".

[15] "Cabinet decision (No. 501) approving the List of Critical Information Infrastructure Objects, avaliable at https://e-qanun.az/framework/58346#_ftn1".

[16] "Directive (EU) 2016/1148 (NIS Directive), Art. 14.".

[17] "Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027, Presidential Decree".

[18] "Convention on Cybercrime (Budapest Convention), ETS No. 185, Arts. 2–21.".

[19] "UN Group of Governmental Experts, Report on Developments in the Field of Information and Telecommunications in the Context of International Security (UN Doc A/70/174, 2015), para. 13.".

[20] "Directive 2014/41/EU on the European Investigation Order, Arts. 1–3.".