Research article
UDC 34:004:342.3:004.9
EDN: https://elibrary.ru/sywsrk
DOI: https://doi.org/10.21202/jdtl.2024.14

Demarcation of Cyberspace: Political and Legal Effects of Applying the Concept of Sovereign States' Interests

Yassin Abdalla Abdelkarim
Luxor Elementary Court, Sohag, Egypt

Keywords

border,
cyber interest,
cyber security,
cyber sovereignty,
cyberspace,
digital technologies,
law,
national interest,
sovereignty,
state

Abstract

Objective: to substantiate the existence of national cyber sovereignty as a legal concept; by introducing the concept of state cyber interests as an innovative determinant, to review the traditional concepts of national sovereignty and state borders in the context of the dynamic nature of cyberspace and the need to develop a hybrid mechanism for cyber borders protection, based simultaneously on law and technology.

Methods: the doctrinal method was used to identify the basic discrepancies in the views of leading scientists in different fields on fundamental theoretical-methodological, conceptual and categorical issues, including the justification of a single algorithm for establishing borders in cyberspace. The doctrinal method is supplemented by the analysis of judicial practice of different countries, which allows considering the courts extending their jurisdiction to disputes related to cyberspace.

Results: the study presents the application of traditional and modern legal concepts of sovereignty in the new digital environment, resulting in a combination of legal and technological approaches. The author reveals functional significance of the concept of state cyber interests for demarcating cyberspace and defining the boundaries of national sovereignty. The adaptability of this concept to the technically uncertain nature of cyberspace is shown. The conclusion is made about the main directions in forming the concept of cyber interests in cyberspace and its political and legal implications, based, among other things, on the practice of courts of different countries in resolving cyber disputes.

Scientific novelty: the concept of state cyber interests is considered as an innovative method of defining cyber borders. It leads to the transformation of the traditional sovereignty concept and the close national interest concept in relation to cyberspace in the context of fulfilling security requirements and intensifying national defense against cyber threats.

Practical significance: the obtained results eliminate existing contradictions in the definition of sovereignty and its spatial limits under the modern technology development; contribute to the elaboration of a disciplinary standard of cyber sovereignty based on a reliable demarcator necessary for the definition of state sovereignty and borders in cyberspace; adapt traditional legal concepts of sovereignty and national interests to the global modern cyber challenges; contribute to the transformation of traditional legal concepts of sovereignty and national interests in cyberspace.

For citation

Abdelkarim, Y. A. (2024). Demarcation of Cyberspace: Political and Legal Effects of Applying the Concept of Sovereign States' Interests. *Journal of Digital Technologies and Law, 2*(2), 262–285. https://doi.org/10.21202/jdtl.2024.14

Contents

Introduction
1. Sovereignty and Borders in Cyberspace: Integral Coherence
   1.1. Evolution of Borders and Sovereignty in Cyberspace
   1.2. Cyber Sovereignty Tight Nexus to Nationalism
   1.3. Cyberspace Demarcation: The Need for a Determinant
2. Utilizing the State Interest Concept to Demarcate Cyberspace
   2.1. Demonstrating the Concept
   2.2. The Political and Legal Implications of State Cyber Interest Concept
   2.3. The Judicial Interpretation of State Cyber Interest Concept
3. The Applicability of the State Interest Concept to Demarcate Cyberspace
   3.1. Applicability Foundations
   3.2. Demarcation Practical Framework
Conclusions
References

Introduction

The inauguration of the Internet has opened an ultimate unbounded sphere of interactions which extends universally. Nowadays, cyberspace connects each corner of Earth. This permits cosmopolitan multi-directional streams of data among nations that transfer a diversity of information, constituting international human cyber interactions.

The borderless theme of cyberspace challenged traditional legal norms of sovereignty and borders, which are indispensable to imposing state control over national territory to deter extraterritorial harm caused by countless foreign illegal cyber activities. Thus, security requirements implied reconceptualizing those notions in cyberspace to activate a national shield against cyber threats. As a response, scholars competed to elaborate on these concepts in cyberspace. They sought to imagine a clear portrait of them and develop firm standards to determine their manifestation in cyberspace. Nevertheless, the absence of a unified methodology created contradicting portraits of sovereignty and borders in cyberspace according to the scope of each scholar. Consequently, they differed in presenting the required determinant.

Henceforth, the research allocates this practical gap and tries to bridge it by introducing a new determinant of sovereignty and borders concepts in cyberspace. This determinant is the concept of state cyber interest. The research points out that national interests in cyberspace are the chief motivation for state intervention. State interests are the true presentation of nationalism in cyberspace; they drive states to act to safeguard their sovereign interests.

To achieve the research objective, it reviews relevant literature on sovereignty and borders in cyberspace to prove their integral coherence and their tight link to the idea of nationalism. Then, it sheds light on the absence of a disciplined demarcation standard in cyberspace, which is the practical gap in knowledge that the research seeks to bridge. Afterwards, it explains the concept of state interest and previews its implications and how domestic courts utilise it to settle cyber disputes. At last, the research proves the functionality of the state cyber interest concept to assign borders in cyberspace through legal reasoning and providing a practical framework.

1. Sovereignty and Borders in Cyberspace: Integral Coherence

As a legal political notion, sovereignty has been a controversial concept that jurists and politicians have elaborated on since the 16th century. It is a crucial organizer of inter-state relations and the entire global motion of human interactions. Prominent Western scholars like Bodin[1] and Hobbes[2] portrayed sovereignty as the king's ultimate authority

[1] Jean Bodin (1530–1596), a French politician and Philosopher.

[2] Thomas Hobbes (1588–1679), English philosopher, scientist, and historian.

to make decisions within a nation[3] According to their view, sovereignty is a political determinant of state power over a bordered territory; a limitation of national power that imposes a de facto obligation of mutual respect of national sovereignty among states. This political notion evolved into a social contract according to Rousseau[4]. Afterwards, philosophers and jurists developed sovereignty theories. Regardless of the various explanations of sovereignty, it remains a core determinant of state authority over its territory according to the Westphalian doctrine, sovereignty refers to the supreme power of a state within a territory (McLean & McMillan, 2009). This concept is the traditional definition of sovereignty in legal and political sciences that suits the nature of inter-state interactions in the real world. Thus, states adopt traditional demarcation methods to draw the national borders among them that regulate their powers and interactions.

Nevertheless, the emergence of cyberspace as a modern sphere of human relationships and interactions implied stretching the traditional notions into its cyber activities. This fact demanded that jurists and scholars rethink their attitudes toward the existing notions and theories to fit cyberspace. Therefore, the concept of sovereignty began to crystallize in cyberspace to organize state power and track illegal activities. Because of the glaring differences between cyberspace and the real world, academics and legislators exert tremendous endeavours to reshape sovereignty under the dynamic nature of cyberspace. The reshaping process proved the uselessness of the traditional border demarcation methods due to the distinguishing nature of cyberspace. The latter implies the development of a specific appropriate tool to draw cyber borders that determine states sovereignty.

In this section, the study explores the evolution of the literature on the concepts of cyber sovereignty and cyber borders to grasp the scholarly efforts of reshaping sovereignty. Then it reviews the social and political perspectives of cyber sovereignty to determine its impacts on national politics and domestic social policies, shedding light, in particular, on the legislative aspect. Last, the study analyzes the demarcation process in the real world and cyberspace to disclose the vacuum in determining state sovereignty in cyberspace.

1.1. Evolution of Borders and Sovereignty in Cyberspace

In 1983, the official open worldwide communication sphere “the Internet” was introduced to humanity (University System of Georgia Online Library) thanks to the invention of the Transfer Control Protocol/Internetwork Protocol (TCP/IP). Since then, massive amounts of data have been transferred globally among Internet users, who

[3] Sovereignty. (2024, Mar. 12). Encyclopedia Britannica. https://clck.ru/3A7Ttf

[4] Jean-Jacques Rousseau (1712–1778), a French Philosopher.

were individuals, entities, and governments. The development in data exchange drove scholars to analyze the newly invented sphere of interactions to conclude its features.

Choucri and Clark pointed out that the absence of sovereignty in cyberspace is not imagined (Choucri & Clark, 2013); traditional sovereignty extends to cyberspace but in a form that suits the borderless nature of this sphere. They mean that sovereignty should be contextualised according to the technical nature of cyberspace. This solution manifests an attempt to integrate a legal notion into a technical context to overcome the legal vagueness of cyberspace.

Scholars continued to develop a clear understanding of cyber sovereignty by creating a discipline determinant of this concept. Therefore, they focused on explaining and clarifying how borders are manifested in cyberspace. Borders are the logical corollary for sovereignty because they constitute its boundaries. Sovereignty and borders are twin concepts; to determine sovereignty borders should be disciplined and allocated. This logic stretches to cyberspace as the accurate interpretation of sovereignty requires developing a disciplined determinant of borders in cyberspace.

Henceforth, scholars sought to innovate a technical determinant of national borders in cyberspace. These borders share the same features and functions as traditional borders since they enable states to impose their sovereignty in cyberspace. Accordingly, Osborn defined cyber borders as the "Functional Equivalent of the Border, where the data arrives at the first practical point of inspection — a network router, computer server, PC, or other networked devices" (Osborn, 2017). His definition is based on the explanations of data exchange models provided in his research. As a consequence, state authorities, e.g., customs officials, can observe data flow in cyberspace to track illegal merchandise or to impose taxes on other legally traded cyber materials. The prominence of Osborn's definition is caused by his bias toward a purely technical approach in explaining a legal notion, that suits the nature of cyberspace. He considered that state cyber sovereignty extends to the first point where data flow interacts with state interests. Likewise, Fang prioritized the technical aspect when defining cyber sovereignty by stating "Cyberspace sovereignty of a state is based on the ICT (Information and communications technology) systems under the state's own jurisdiction; the boundaries thereof consist of a collection of the state's own network device ports directly connected to the network devices of other states; cyberspace sovereignty is exercised for protection of various operations of data by cyber roles" (Fang, 2018). He drew the state cyber territory according to its national network of devices. Therefore, the network map is the state territory in cyberspace. Furthermore, he mentioned that cyber sovereignty grants the state the same powers over its territory granted by traditional sovereignty, e.g., self-defence and independence (Fang, 2018). Fang's definition is a successful mixture of law and technology because it established state territory in cyberspace on the technical map of national network devices and mentioned state rights granted by this legal concept.

In this regard, the Egyptian Public Prosecution adopted a functional approach concerning the admittance of cyber borders. An official statement noted that the state has virtual borders in cyberspace; they manifest the fourth political state boundaries[5]. Thus, surveilling this sphere of interactions constitutes a state interest of utmost importance. Despite the statement devoid of a definition of cyber borders, it admitted their existence and functions.

The Internet occupation of modern-day life intensifies human relations and interactions in cyberspace. The ongoing developments of cyberspace communication techniques challenge states power to impose order on the Internet. These developments motivated modern scholars to sharpen their lens on the legal issues that arise from cyber interactions. Among these issues, the questions of state sovereignty and its national authority over cyber territory have occupied a considerable position in scholars' debate. In addition, jurisprudence developed several tools to assign political borders in cyberspace.

Cyber sovereignty should not be limited to the physical perspective of network devices (Omar et al., 2022). The absence of traditional borders in cyberspace implied conceptualizing sovereignty to adapt to the technical unbounded nature of cyberspace. Therefore, Omar et al. introduced the term "Universal Information Sovereignty" to express the state authority to conduct cyber security operations to defend its national interests in virtual reality (Omar et al., 2022). They argued that determining the limits of state cyber sovereignty is a political process rather than legal because each state has its own evaluation of data flow and its effects on national interests (Omar et al., 2022). They shed light on the practical aspect of cyber sovereignty by figuring out its direct nexus to cyber security. Sovereignty is the legitimization of cyber security operations. Thus, it is an ultimate manifestation of state interests in cyberspace.

Zekos noted that the global nature of the Internet transferred the practice of sovereignty from states to market forces because this nature replaces the traditional interpretation of state sovereignty with a globalized market power that accords the capitalist control of cyberspace (Zekos, 2022). Due to the ongoing economic benefits of globalized cyberspace, states suffer hardships regarding securing their traditional sovereignty (Zekos, 2022). Therefore, cyber globalization created the concept of cyber sovereignty; it is an adaptation of the traditional legal notion of sovereignty in cyberspace (Zekos, 2022). Cyber sovereignty, hence, suits the boundlessness of the cyber sphere, where traditional territorial boundaries disappear entirely. Nonetheless, he claimed that state sovereignty, in its legal concept, has a strong nexus to its territory as this notion permits the state to impose its authority within the national borders (Zekos, 2022). Accordingly, he

[5] The Egyptian Public Prosecution. (2020). Official Statement on Hanin Hossam's Case. https://clck.ru/39rfJM

stipulates the existence of a recognized state territory in cyberspace to establish its sovereignty over it. With the absence of traditional territorial boundaries, he suggested applying advanced geographical digital tracking of data flow on the Internet to ensure state sovereignty (Zekos, 2022). Furthermore, he concluded that states should adopt the effect factor to recognize their territory in cyberspace (Zekos, 2022); each activity that generates effects within the traditional territory extends state sovereignty over it. Under this interpretation, domestic courts managed to establish personal jurisdiction over cyber disputes. The nexus between the cyber society and the state justifies stretching national sovereignty to cyberspace, disregarding the distinguishing cyber dimensional expression (Zekos, 2022). Consequently, states can impose their sovereignty over electronic transactions and interactions that affect their interests. This elaboration proves the existence of cyber sovereignty as a legal notion.

According to Simmons and Hulvey, imposing cyber borders implies paving the road for domestic laws to organize and control data flows between national cyber spatial and universal cyberspace (Simmons & Hulvey, 2023). Henceforth, cyber borders reflect the governments' endeavours to control national cyberspace against foreign interference (Simmons & Hulvey, 2023). Thus, borders and sovereignty are two sides of a single coin in cyberspace, which is national security.

Respecting cyber sovereignty is a chief principle concerning cyber operations. It is an extension of traditional sovereignty which constitutes a threshold of peaceful global cyber cohabitation (Japaridze, 2023). Cyber sovereignty provides states with the authority to surveil and track illegal activities on the Internet and to take the appropriate countermeasures to maintain their national integrity in the virtual world (Japaridze, 2023). Thus, cyber sovereignty contributes to protecting individuals against cyber threats. However, the extremist interpretation of cyber sovereignty might Balkanize cyberspace to tiny distant islands (Japaridze, 2023), which contradicts the original purpose of this global sphere. Hence, sovereignty, as a determinant of state authority, is indispensable in cyberspace to organize global interactions.

It is worth mentioning that Zein defined cyber sovereignty as "the submission of cyberspace to state interests and values" (Zein, 2022). This definition implies the state ultimate authority to control and surveil cyberspace and reflects the obvious nexus between sovereignty in cyberspace and state authority. It also includes the exerted efforts to demarcate cyberspace. She argued that cyberspace is a de facto "universal common" similar to international high seas and human cultural heritage (Zein, 2022). Therefore, it is challenging to impose certain state sovereignty over it. Nevertheless, states might crystalize their national cyber sovereignty by imposing technical measures to limit data flow, observe suspicious activities, and exploit the vagueness of cyberspace against other states (Zein, 2022). Furthermore, the legal consequences of traditional sovereignty

extend to cyber sovereignty because states should consider mutual respect for national sovereignty while operating in cyberspace, avoiding unlawful interference in the internal affairs of other countries, and maintaining the integrity of territorial cyber sovereignty against illegal cyber attacks that target critical infrastructure (Zein, 2022). It should be noted that Zein highlighted that cyber sovereignty has a strong nexus to state security and well-being. The political perspective overwhelms her elaboration on stretching sovereignty, in its traditional legal interpretation, to the newly innovated cyberspace. In this context, Zhuk argued that sovereignty in cyberspace is purely virtual and implies imposing state control over its digital infrastructure located within the national virtual territory (Zhuk, 2023). It is an exclusive feature of online communities that has no ties with traditional physical territory.

To sum up, since sovereignty legitimizes state actions to defend national interests, scholars spared no effort to elaborate on how this concept is manifested in cyberspace. While old scholars debated its existence, modern literature discloses the global admittance of cyber sovereignty. This acceptance is evident in the scholarly endeavours to interpret this notion within the technical context of cyberspace. It is crucial to note that scholars managed to highlight the functional aspects of cyber sovereignty when explaining it; their definitions reflected that sovereignty is the method that legitimizes state practices in cyberspace to present its national interests. Furthermore, the absence of a clear determinant of sovereignty might trigger a global cyber conflict because of inter-state authority overlapping. This consequence threatens the stability required by the flourishment of universal interactions in cyberspace. Therefore, the development of a discipline determinant of cyber sovereignty is a must to evade dire consequences.

1.2. Cyber Sovereignty Tight Nexus to Nationalism

Nationalism has become the chief determinant of state perceptions of spaces since its evolution in the 18th century. States managed to control their spaces on the basis of national interests. Koulos argued that countries, to exercise their powers within a specific territory, initiate a nationalization process of it (Koulos, 2022). According to Cox, nationalism is "the sum of those beliefs, idioms, and practices, oriented to a territorially delineated nation and embodied in the political demands of a self-identified people, which may or may not be realized in a nationalist movement and state 'of their own'" (Cox, 2021). From this definition, it could be understood that nationalism had been limited to traditional territorial spaces for a while. Nonetheless, the emergence of the Internet eliminated the traditional boundaries between nations and permitted transnational interactions. Therefore, nationalism evolved to conquer cyberspace as states inaugurated plans for the nationalization of cyberspace. In this aspect, the research explores the strong links

between sovereignty and nationalism in cyberspace as a threshold to prove the need to demarcate states cyber sovereignty and find a determinant of states cyber borders. Moreover, it sheds light on certain states regulations of cyber security to reveal the national attitudes toward cyberspace demarcation.

The sense of nationalism does not suppress its application to the real world; on the Internet, several interactions are motivated by nationalism. The unlimited universal nature of cyberspace created several fields of digital rivalry. The controlling factor of this rivalry is nationalism. Therefore, despite its ambiguous nature, states sought to incorporate cyberspace into their national concepts (Koulos, 2023). Put differently, national regimes would try subordinating cyberspace to their political ambitions. For instance, the URL terminus usually refers to the state where the domain owner is located, e.g., .fr for France, .us for the United States, and .eg for Egypt. Koulos brought this instance as preliminary evidence of cyberspace nationalization. The global theme of cyberspace evolved a cosmopolitan understanding of nationalism because of the reshaping of values (Cox, 2021). Globalization aroused national political ambitions for domination in cyberspace. Henceforth, Cox indicated that a borderless sphere ignites fevered inter-state competition under the flag of nationalism (Cox, 2021). Furthermore, borders in cyberspace are shaped to protect sovereignty over national soil. Nonetheless, states utilize appropriate techniques to impose national cyber borders. These mechanisms suit the specific technical vague nature of cyberspace, distinguishing them from the traditional border demarcation methods. The intensive globalization of cyberspace drives states to concentrate on its territorialization to safeguard their national interests against political tensions[6]. Nationalism is the main justification for their policies.

Since cyberspace is a rich well of data, superpowers seek to impose their control on it under the notion of cyber sovereignty[7]. Therefore, states utilize specific technologies to strengthen their grasp on the national cyber territory. They impose national sovereignty in cyberspace through data observance and capture mechanisms to maintain cyber superiority as a part of an overall economic and security plan (St-Hilaire, 2020). States might use their political pressure on Internet giants to exploit their technical capabilities within political conflicts[8].

6 Benabid, M. (2022, August). The Territorialization of Cyberspace and GAFAM Geopolitics: Driving Forces and New Risks in the Wake of the Ukrainian Crisis. Policy Brief. № 52/22. https://clck.ru/3A7YMR

7 Ibid.

8 Blenkinsop, Ph. (2022, March 3). EU bars 7 Russian banks from SWIFT, but spares those in energy. Reuters. https://clck.ru/3A7Yt8

Furthermore, Cyberspace has become a major inter-state confrontation field because of the variety of contradicting interests the flowing data represents (Manshu & Chuanying, 2021). These cyber conflicts might trigger political situations with dire consequences if not settled. In practice, it is witnessed that states like China and Russia invested enormous deals of technology to establish their patriotic sovereignty in cyberspace to enhance their cyber security against the domination of Western countries. Even though their policies might Balkanize cyberspace, which contradicts free data flow, these states prioritize national interests (St-Hilaire, 2020). Nationalism is the glaring engine of these policies, evidencing its strong nexus to cyber sovereignty. A prominent example of the nexus between cyber sovereignty and nationalism manifests in Hillary Clinton's promise to eliminate the digital Iron Curtain deployed by China to control data flow on the Internet (St-Hilaire, 2020). It is an inter-state cyber competition for domination motivated by nationalism to guarantee national cyber supremacy. Moreover, the US Cyber Command was established to function as a task force protecting the national US interests in cyberspace against foreign threats[9]. Afterwards, the Chinese President declared, in 2014, the national vigorous endeavour to gain supremacy in cyberspace (Segal, 2014). Nationalist competitions to dominate cyberspace manifests a techno arms race between superpowers to hold strongly this wealthy data resource.

To conclude, wealthy cyberspace ignited states enthusiasm to dominate this sphere of interactions. They are motivated by nationalist ideals of supremacy to guarantee national outperformance in cyberspace. This fact implies states endeavour to impose borders in cyberspace to safeguard national interests and defend sovereignty. Through these endeavours, the concept of nationalism is represented in cyberspace, which proves its strong tie with cyber sovereignty. Indeed, defending national cyber borders prerequisite to developing a mechanism to assign these borders in cyberspace.

1.3. Cyberspace Demarcation: The Need for a Determinant

The previous review reveals that jurisprudence admitted that assigning borders in cyberspace is indispensable to determining the limits of national sovereignty for evading potential confrontations. The existence of cyber borders is the core of cyber sovereignty which grants their demarcation a distinguished importance. In the real world, the demarcation of inter-state borders does not constitute an obstacle because states utilize the traditional tools adopted and affirmed by international law. Furthermore, nationalist motivations imply assigning obvious state borders to enable national defence in cyberspace. Nevertheless, because of the technically ambiguous nature of cyberspace, the process of assigning national borders becomes prominently complicated.

[9] Command (2010), Our Mission and Vision. https://clck.ru/3A7XsQ

It is affirmed that the state territory is the spatial of its exclusive authority, which is bounded by admitted and clear boundaries that constitute the state political borders (Ahmed, 2021). Traditionally, borders indicate the extent to which a state can impose its authority. Thus, demarcating obvious borders between states and territories is crucial for stability and peace; it prevents unlawful interference among nations. Since a state without a territory is not imagined, a territory without borders cannot exist because the integrity and acceptance of a territory depends on assigning its obvious and stable borders. Traditional borders are maintained by techniques under authorization legal chains that surveil the physical movement of persons and goods, e.g., entry and departure visas, customs administration, and frontier and coast guard units (Simmons and Hulvey 2023).

Likewise, cyberspace demarcation occupies a prominent order in protecting state interest policies. States have a legal right to impose their sovereignty against cyberattacks targeting national infrastructure. Furthermore, cyber sovereignty is a chief concern regarding criminal justice because of the obligation of the national judicial authorities to respect other state sovereignty while gathering evidence on the Internet (Sallavaci, 2020). Cross-border judicial proceedings should be organized by multilateral, or bilateral, treaties to avoid violating cyber sovereignty. Therefore, contemporary scholars admit that cyber sovereignty is required for criminal justice. This fact requires innovating an appropriate mechanism to assign borders in cyberspace. Nevertheless, the rapid dynamic environment of cyberspace as a consequence of the tremendous universal data flows complicates assigning clear political borders (Abdelrahman & Mekhiemer, 2022). Restricting the national territory in cyberspace to a limited space is a complicated idea because of the lack of a disciplined determinant, contrary to traditional borders. Traditional interstate borders have become unrealistic because of the global theme of cyberspace (Ahmed, 2021).

To border the national cyber territory, states use their traditional territorial metaphors to respond to foreign cyber threats (Simmons and Hulvey, 2023). This approach is motivated by the states spatial thinking of cyberspace. They consider cyberspace a territory to dominate where they practice sovereign control. Techniques like data localization, website blocking, and judicial cooperation requests are symbols of combining technologies and law to demarcate cyberspace. Osborn's definition of cyber borders reflected this attitude. However, depending on a technical pillar to impose a firm border in cyberspace might prove deficient because of the rapid developments of Internet technologies that might confront slow legislation amending process. Thus, it becomes urgent to develop a stable determinant of cyber borders. This research introduces the concept of state interest as a determinant of cyber borders.

2. Utilizing the State Interest Concept to Demarcate Cyberspace

2.1. Demonstrating the Concept

The concept of human interest refers to the needs which persons seek to satisfy for their well-being. These needs are not purely singular but they have social specifications resulting from their contributions to social relations. Moreover, they are not absolute because of production capabilities restrictions (Wang, 2022). Through their pillars, interests manifest the social transformation of human needs and the tight tie binding humans together in a specific field of interactions. They are determinants of human relations that unify them in certain situations and diverse them in other situations. Because of the diversity of interest factors, they can create contradicted positions among social groups, i.e., states (Wang, 2022). Interests are the starting points for creating political, economic, and social ties within a community (Wang, 2022). Cox (2021) argued that interests have become the main pillar of social sciences concentration because of their contribution to the concept of collective emotions in a community (Cox, 2021). Thus, interests are the effective expression of the collective motivation of a group that drives national authorities to react for protection.

Concerning states, interests as a social phenomenon refer to national requirements that satisfy domestic needs against the interests of other states. Since states might differ in their interest identification standards, conflict of interests occurs. Therefore, interests determine the way that states behave to guarantee their needs. Applying this meaning in cyberspace implies that each state would conduct itself to satisfy its national needs on the Internet; states cyber behaviour will be conducted according to their interests.

States interests are common interests because they are formed by the needs of a united group (Wang, 2022). In cyberspace, the concept of state interest, as a common interest, has main characteristics; publicity, realization through the chain of product supply, unity, fundamental values inclusion, and independence (Wang, 2022). These are the chief determinants of state interest as a concept.

2.2. The Political and Legal Implications of State Cyber Interest Concept

Fang argued that national sovereignty in cyberspace is a political state interest (Fang, 2018) and when a state imposes its authority over its cyber territory it defends national cyber interests. Put differently, assigning political borders in cyberspace and tightening national sovereignty within them reflects a utilization of the state interest concept to determine and maintain cyber borders. Another example of subordinating state cyber diplomacy to state interest is the contradiction between the US and China.

While the US fights for unlimited cyberspace because achieving national interests demands the free flow of data, China tends to impose strict cyber borders to defend cyber independence (Fang, 2018). This instance highlights the critical impact of the interest concept on state cyber policies. States can enforce data processing to ensure the legitimacy of exchanged data within their cyber borders and to track illegal cyber activities (Paice & McKeown, 2023). This practice enhances the integrity of the national cyber terrain and the true concept of cyber sovereignty. It is a critical contribution of the state interest concept to securing cyber borders. In particular, state interests are the chief motivation for nationalism in cyberspace (Cox, 2021); wherever a state cyber interest is threatened, a national intervention becomes obligatory to defend the integrity of national benefits. This conclusion accords with the core of sovereignty and nationalism in cyberspace. Furthermore, threatening state cyber interests triggers cyber warfare which includes mutual cyberattacks across states cyber borders to defend national economic and military facilities (Fang, 2018). Threats to cyber interests demand urgent state reactions to confront them, protecting national interests.

In 2024, a US Report pointed out the urgent need to draft a clear cyber diplomacy to protect state interests in cyberspace[10]. This report presented an official governmental admittance of the state cyber interest concept and utilized it to plan national diplomacy in cyberspace. Consequently, the concept of state cyber interest is affirmed in politics and diplomacy. Likewise, the EU adopted joint cyber diplomacy, which maintains the collateral cyber interests of the EU (Reiterer, 2022). He encouraged the EU to adopt the most advanced technologies to protect cyber interests against the ongoing growth of competitive cyber powers (Reiterer, 2022). Cyber interests have become a prominent element in drafting national grand strategies.

From a legal perspective, it is admitted that cyberspace is a virtual sphere of global interactions that generates real relations among nations. Cyber interactions cause impacts on human relations in the real world. This fact triggers the need to regulate cyberspace, providing a legal framework for these interactions (Fang, 2018). Thus, states impose their legislation in cyberspace to protect their national interests.

2.3. The Judicial Interpretation of State Cyber Interest Concept

Contextualizing the concept of state cyber interest is not solely rhetoric because studying case laws, including cyber litigations, figures out how national judiciaries utilized this concept to settle cyber disputes.

[10] US Government Accountability Office. (2024, January). Cyber Diplomacy. State's Efforts Aim to Support U.S. Interests and Elevate Priorities: Report to Congressional Addressees. https://clck.ru/3A7Y99

The US judiciary confronted the threat of online child pornography in State v. Hunt (2020) to defend American society. Their rulings were based on the gravity of exploiting minors in this heinous behaviour. Therefore, the court claimed that the possession of pornography materials expresses the defendant's criminal intent to view it according to 18 U.S.C. § 2252A. The judgment reflects that a state cyber interest, i.e., eliminating online child pornography, led the court to impose national legislation in cyberspace. Likewise, in People v. Jacobo (2019) the court applied the US definition of online human trafficking under the permission to prosecute this criminal actus reus universally granted by the Californians Against Sexual Exploitation Act (the CASE Act 2012) for law authorities to prosecute these activities if a US citizen is involved. It is a clear extension of the US cyber borders because the state interest requires this. The judicial shield is manifested in the US court intervention to protect the integrity of the electoral regime in Democratic Nat'l Comm. v. Russian Fed'n (2019) against foreign cyber attacks that threatened the whole US democratic system. Furthermore, economic state cyber interest was valid to initiate judicial proceedings to defend as in REGINA v CORY AGUILAR (2018); a UK court indicated that harm inflicted on the plaintiff by the defendant's cyber money fraud activity sufficed to imprison him upon found guilty. In addition, The UK judiciary countered internet smuggling in Regina v Stephen Brownlee (2020). The court approved targeting undisclosed websites that were used by smugglers as platforms of illegal goods exchange. The judgment considered these websites as state borders' penetration spots and permitted taking them down to protect national interests.

Defending national creativity, the UK judiciary confronted illegal online trade in unlicensed materials or artworks in Lifestyle Equities CV v Amazon UK Services Ltd. (2021) and Tunein Inc v Warner Music UK Limited, Sony Music Entertainment UK Limited (2021). Needless to say, unoriginal materials inflict moral and financial harm to patent owners whose protection manifests a critical state interest under the UK Copyright, Designs and Patents Act 1988.

Defending society against rumours, American judge O'Scannlian considered an inaccurate online business report in Robins v. Spokeo (2017) a violation of the US Fair Credit Reporting Act that grants the plaintiff the right to compensation. Similarly, the UK court admitted the same right in Ghannouchi v Middle East Online Ltd & Anor (2020). Thus, it confronted the spread of fake information on the websites defending the credibility of the national press.

To conclude, the previewed judgments reveal that judiciaries admitted the existence of the cyber borders concept by connecting it to the concept of state interest. This functional interpretation means that the state cyber borders are assigned according to the state interests in cyberspace; wherever an interest exists, states can extend their cyber sovereignty to defend it. Nonetheless, the judgments do not introduce a normative definition of cyber borders; the interests that they defended on the internet are the state's cyber borders according to the functional interpretation which accords with Osborn's (2017) and Zein's (2022) definition.

3. The Applicability of the State Interest Concept to Demarcate Cyberspace

3.1. Applicability Foundations

Needless to say, cyberspace still lacks a firm determinant of borders concept. States utilize several mechanisms to safeguard their national interests. The diversity of cyber domestic policies contradicts the universality of cyberspace which stability requires a unified set of normatives. The absence of multilateral conventions on cyberspace demarcation, the competitive political cyber interests, the diversity of national interpretations of legal notions, and the establishment of attribution and accountability in cyberspace are the chief odds before adopting a global determinant of cyber borders concept[11]. With the absence of a legal demarcator, the research introduces the notion of state interest as the required determinant of the cyber borders concept.

As a global common, cyberspace requires a universally admitted standard to assign political borders. Keep in mind that the pure technical nature of cyberspace does not prevent the contextualization of legal notions within its sphere. The traditional concept of sovereignty stretches to cyberspace, but in a form that complies with its technical theme (Choucri & Clark, 2013). Combining law and technology was the major odd that stood before scholars' endeavours to develop a normative to demarcate cyberspace. This odd drone Osborn to adopt an ultimate technical approach to define cyber borders as previously shown. Nevertheless, the scholarly evolution discloses the prominent approach to link borders and sovereignty concepts in cyberspace to the state interest concept.

Adaptability is the key to the successful integration of a legal notion into a digital environment (Akhmatova & Akhmatova, 2020). It is the challenge that stands before cyberspace legalization and governance. The adaptability of the state interest concept to the technical vague nature of cyberspace is glaring. Since cyberspace is full of different categories of human needs, the concept of interest is crystallized in the methods adopted by nations to satisfy those needs. As Wang (2022) indicated, interests are the true expression of social life among communities; they are the engine of human social interactions. Therefore, they should be prioritized when assigning boundaries and limits between groups. Therefore, the concept of state interests in cyberspace has evolved to formulate the threshold of state cyber policies. The adaptability of its pillars with cyber interactions qualifies this concept to be employed as a determinant of state authority in cyberspace.

[11] Hollis, D. B. (2021, June). A Brief Primer on International Law and Cyberspace. Carnegie Endowment for International Peace. https://clck.ru/3A7ZPU

Furthermore, national interests are the chief motivations for states intervention in cyberspace. Studying the Chinese and Western approaches discloses their hastened endeavours to crystallize their cyber sovereignty according to the national interests they plan to safeguard in cyberspace. In particular, the firm presence of nationalism in cyberspace motivates states to utilize their domestic legal toolkits to defend their cyber interests. Based on Benabid's[12] and Paice and McKeown's (2023) analysis, states interests are the active engines of national policies in cyberspace. These facts prove the national prioritization of state cyber interests, which are reflected in the political implications of this concept.

From a judicial perspective, the judgments of national courts in cyber disputes qualify the state interest concept to assign cyber borders. The US and UK judiciaries extended their jurisdiction in cyberspace wherever a national interest is threatened. Since jurisdiction manifests sovereignty, domestic courts impose national sovereignty to the extent that state interests are affected. This judicial interpretation employs the state interest concept as a determinant of state cyber sovereignty and, consequently, borders.

3.2. Demarcation Practical Framework

After establishing the legal foundation to utilize the concept of state cyber interest to determine cyber borders, it is obligatory to develop a practical framework for this process otherwise the whole establishment becomes fruitless. The article introduces several methods to employ this concept as a boundary determinant.

Because of the universality of cyberspace, scholars suggest using international law mechanisms through conventions and developing customary international law to support the adaptability of pure legal notions to the technical nature of cyberspace[13]. Thus, states should tend to sign conventions on adopting the state interest concept to assign cyber borders. Regulating universal cyberspace requires universal mechanisms because unilateral policies might jeopardize global regulation endeavours. In addition, multilateral understandings ensure international consensus on adopting state cyber interest as a demarcator in cyberspace. As a consequence, the concept of state cyber interest achieves disciplinary that enhances its contribution to cyberspace governance.

---

[12] Benabid, M. (2022, August). The Territorialization of Cyberspace and GAFAM Geopolitics: Driving Forces and New Risks in the Wake of the Ukrainian Crisis. Policy Brief. № 52/22. https://clck.ru/3A7YMR

[13] Hollis, D. B. (2021, June). A Brief Primer on International Law and Cyberspace. Carnegie Endowment for International Peace. https://clck.ru/3A7ZPU

Innovation is the key to overcoming techo-legal dilemmas (Linden & Shirazi, 2023). Scholars need to develop their traditional interpretation of legal notions to adapt them to technical environments like cyberspace. Moreover, innovation is a pillar of modern cyber operations because it grants states advantageous opportunities in cyberspace (Soare, 2023). In the judicial field, domestic courts combined technical tools with traditional legal notions to overcome the technical nature of cyber disputes. It is a unique mechanism to protect cyber borders, which has two pillars: law and technology. This hybrid structure provided that mechanism with flexibility that adapted legal concepts to technical cyberspace. Furthermore, flexibility enhanced the national courts' ability to counter cyber threats. Innovation is the key that enabled the judges to overcome the technical odds of cyber disputes and legislation stagnation by combining law and technology.

Handling a discourse with rapid leaps implies transcending realities to tackle obstacles. Therefore, depending solely on realistic logical reasoning to settle the techno-legal dilemma drives jurists to a standstill. In this case, imagination offers a critical contribution to pushing forward legal doctrine. In the legal aspect, imagination provides scholars with impressive, persuasive, and innovative opportunities to overcome traditional obstacles (d'Aspremont, 2022). Legal imagination constitutes a powerful tool against legal bureaucracy; it is "a thinking of the impossible for the sake of resistance" (d'Aspremont, 2022). Furthermore, imagination, from a legal perspective, enhances jurists' capabilities to reconceptualize existing norms within flexible technological environments, where changes occur rapidly and randomly (Pollicino, 2020). Thus, legal imagination enables scholars to develop traditional legal notions to suit the rapidly evolving technical spheres like cyberspace. It should be noted that the concepts of borders and sovereignty were imagination which scholars and courts had successfully interpreted and incorporated within realistic legal contexts through innovative techno-legal principles included within their judgments and interpretations. Likewise, the concept of state cyber interests, through legal imagination, could be contextualized effectively in cyberspace to assign borders and sovereignty. The aforementioned judgments adopted this concept to determine the scope of national jurisdiction, which manifests a direct implication of state sovereignty within national borders. Consequently, it could be concluded that the state cyber borders extend to each spot in cyberspace where a state interest is affected. This interpretation reflects the flexibility of the state interest concept that suits the vague nature of cyberspace where rigid norms are technically jeopardized. Thus, imagination resurrects traditional legal notions in cyberspace by granting them the effective feature of adapting to cyberspace, which is flexibility.

Conclusion

In summary, cyberspace has proven resistant to boundary imposture through traditional demarcation methods adopted to demarcate borders in the real world. Scholars sought to portray sovereignty and borders in cyberspace; the diversity of their attitudes created contradicting understandings of these concepts in cyberspace. Indeed, this contradiction destabilizes universal cyber relations. To overcome this dilemma, the research seeks to develop a modern legal mechanism to determine sovereignty and borders in cyberspace.

Unlike scholarly endeavours, this study adopts a pure legal notion to determine a technical concept. It presents the concept of state cyber interest as the cyberspace demarcation tool. The utilization of this concept implies imposing national sovereignty in cyberspace according to any effect on national interest. Ensuring the functionality of the state interest concept, the research sheds light on its adaptability to the technical nature of cyberspace to transcend traditional odds before integrating a pure legal notion into a technical environment. Furthermore, the required mechanisms to employ this concept have been elaborated on to defend the applicability of this article hypothesis.

References

Abdelrahman, M. A., & Mekhiemer, O. F. (2022). Cyberspace and its Impact on the Concepts of Power, Security and Conflict in International Relations. *Journal of Politics and Economy*, *16*(15), 423–443. (In Arabic). https://doi.org/10.21608/jocu.2022.134235.1172

Ahmed, B. S. (2021). The Role of the International Court of Justice in Resolving International Borders Disputes. *Humanitarian and Natural Sciences Journal*, *2*(6), 632–646. (In Arabic).

Akhmatova, D., & Akhmatova, M. (2020). Promoting Digital Humanitarian Action in Protecting Human Rights: Hope or Hype. *Journal of International Humanitarian Action*, *5*, 6. https://doi.org/10.1186/s41018-020-00076-2

Choucri, N., & Clark, D. D. (2013). Who Controls Cyberspace? *Bulletin of the Atomic Scientists*, *69*(5), 21–31. https://doi.org/10.1177/0096340213501370

Cox, L. (2021), *Nationalism: Themes, Theories, and Controversies. Palgrave Macmillan*. https://doi.org/10.1007/978-981-15-9320-8

d'Aspremont, J. (2022). Legal imagination and the thinking of the impossible. *Leiden Journal of International Law*, *35*(4), 1017–1027. https://doi.org/10.1017/s0922156521000637

Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-0320-3

Japaridze, T. (2023). Cyber Sovereignty: Should Cyber Borders Replicate Territorial Borders? In J. Berghofer, A. Futter, C. Häusler, M. Hoell, & J. Nosál (Eds.), *The Implications of Emerging Technologies in the Euro-Atlantic Space* (pp. 209–225). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-24673-9_13

Koulos, Th. (2022). A Digital Territory to be Appropriated: The State and the Nationalization of Cyberspace [version 2; peer review: 2 approved]. *Open Research Europe*, *1*, 119. https://doi.org/10.12688/openreseurope.14010.2

Linden, T., & Shirazi, T. (2023). Markets in Crypto-assets Regulation: Does it Provide Legal Certainty and Increase Adoption of Crypto-assets? *Financial Innovation*, *9*, 22. https://doi.org/10.1186/s40854-022-00432-8

Manshu, Xu, & Chuanying, Lu (2021). China – U.S. Cyber-Crisis Management. *China International Strategy Review*, *3*, 97–114. https://doi.org/10.1007/s42533-021-00079-7

McLean, I., & McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3 ed.). Oxford University Press. https://doi.org/10.1093/acref/9780199207800.001.0001

Omar, M. O., AlDajani, I. M., Juwaihan, M., & Leiner, M. (2022). Cybersecurity in Sovereignty Reform. In I. M. AlDajani, & M. Leiner (Eds.), *Reconciliation, Heritage and Social Inclusion in the Middle East and North Africa* (pp. 109–128). Springer, Cham. https://doi.org/10.1007/978-3-031-08713-4_8

Osborn, Ph. (2017, October). Cyber Border Security – Defining and Defending a National Cyber Border. *Homeland Security Affairs* 13, Article 5.

Paice, A., & McKeown, S. (2023). Practical Cyber Threat Intelligence in the UK Energy Sector. In C. Onwubiko et al. (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Springer Proceedings in Complexity, Springer, Singapore*. https://doi.org/10.1007/978-981-19-6414-5_1

Pollicino, O. (2020). Metaphors and Judicial Frame: Why Legal Imagination (also) Matters in the Protection of Fundamental Rights in the Digital Age. In B. Petkova, & T. Ojanen (Eds.), *Fundamental Rights Protection Online. Edward Elgar Publishing*. https://doi.org/10.4337/9781788976688.00009

Reiterer, M. (2022). EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacifc. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.). *Cybersecurity Policy in the EU and South Korea from Consultation to Action*. New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2

Sallavaci, O. (2020). Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters. In H. Jahankhani, B. Akhgar, P. Cochrane, & M. Dastbaz (Eds.), *Policing in the Era of AI and Smart Societies, Advanced Sciences and Technologies for Security Applications* (pp 1–58). Springer, Cham. https://doi.org/10.1007/978-3-030-50613-1_1

Segal, A. (2017, June 2). *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Hoover Working Group on National Security, Technology, and Law. Aegis Paper Series, 1703.

Simmons, B., & Hulvey, R. (2023). Cyber Borders: Exercising State Sovereignty Online. *All Faculty Scholarship, 3158*.

Soare, S. R. (2023). Algorithmic power? The Role of Artificial Intelligence in European Strategic Autonomy. In F. Christiano, D. Broeders, F. Delerue, F. Douzet, & A. Géry (Eds.). *Artificial Intelligence and International Conflict in Cyberspace*, Routledge, London. https://doi.org/10.4324/9781003284093-6

St-Hilaire, W. A. (2020). *Digital Risk Governance: Security Strategies for the Public and Private Sectors*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-61386-0

Wang, P. (2022). *Principle of Interest Politics: Logic of Political Life from China's Perspective*. Peking University Press. Springer. https://doi.org/10.1007/978-981-19-3963-1

Zein, M. (2022), The Effect of the New State Sovereignty Concepts on the Jurisdictions of Cybercrime. *International Journal of Doctrine, Judiciary, and Legislation*, *3*(3), 679–738. https://doi.org/10.21608/ijdjl.2022.138565.1159 (In Arabic).

Zekos, G. I. (2022). *Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-94736-1

Zhuk, A. (2023), Virtual Sovereignty: Examining the Legal Status of Micronations in Cyberspace Through the Case of the Republic of Errant Menda Lerenda. *Digital Society*, *2*, 45. https://doi.org/10.1007/s44206-023-00067-x

Author information

Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court, Egyptian Ministry of Justice
Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Conflicts of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – September 21, 2023
Date of approval – October 12, 2023
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:342.3:004.9
EDN: https://elibrary.ru/sywsrk
DOI: https://doi.org/10.21202/jdtl.2024.14

Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств

Яссин Абдалла Абделькарим

Суд общей юрисдикции в Луксоре, Сохаг, Египет

Ключевые слова

государство,
граница,
кибербезопасность,
киберинтерес,
киберпространство,
киберсуверенитет,
национальный интерес,
право,
суверенитет,
цифровые технологии

Аннотация

Цель: обосновать существование национального киберсуверенитета как юридического понятия, наряду с которым путем введения инновационной детерминанты – концепции государственных киберинтересов – переосмыслить традиционные понятия национального суверенитета и государственных границ в условиях динамичной природы киберпространства и необходимости разработки гибридного механизма защиты кибергранниц, основанного одновременно на праве и технологиях.

Методы: на основе доктринального метода выявлены принципиальные расхождения в представлениях ведущих ученых разной отраслевой принадлежности по концептуальным теоретико-методологическим и понятийно-категориальным вопросам, в том числе по вопросу обоснования единого алгоритма для установления границ в киберпространстве. Доктринальный метод дополнен анализом судебной практики разных стран, позволяющим рассмотреть распространение судами своей юрисдикции на споры, связанные с киберпространством.

Результаты: в исследовании представлено применение традиционных и современных правовых концепций суверенитета в новой, цифровой среде, результатом чего стало сочетание правовых и технологических подходов. Раскрыто функциональное значение концепции государственных киберинтересов для демаркации киберпространства и определения границ национального суверенитета. Показана адаптируемость данной концепции к технически неопределенной природе киберпространства. Делается вывод об основных направлениях формирования концепции киберинтересов в киберпространстве, ее политических и правовых последствиях, основанных в том числе на практике судов разных стран по разрешению киберспоров.

Научная новизна: концепция государственных киберинтересов рассматривается в качестве инновационного метода определения кибергранниц, что обусловливает трансформацию смысла традиционного понятия суверенитета и тесно связанного с ними понятия национальных интересов применительно к киберпространству в контексте обеспечения требований безопасности и активизации национальной защиты от киберугроз.

Практическая значимость: полученные результаты устраняют имеющиеся противоречия в определении суверенитета и его пространственных пределов в условиях развития современных технологий; способствуют выработке дисциплинарного стандарта киберсуверенитета на основе надежного демаркатора, необходимого для определения государственного суверенитета и границ в киберпространстве; адаптируют традиционные юридические понятия суверенитета и национальных интересов к глобальным современным кибервызовам; способствуют трансформации традиционных правовых институтов и норм в области суверенитета и границ в условиях киберпространства.

Для цитирования

Абделькарим, Я. А. (2024). Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств. *Journal of Digital Technologies and Law*, *2*(2), 262–285. https://doi.org/10.21202/jdtl.2024.14

Список литературы

Abdelrahman, M. A., & Mekhiemer, O. F. (2022). Cyberspace and its Impact on the Concepts of Power, Security and Conflict in International Relations. *Journal of Politics and Economy*, *16*(15), 423–443. (In Arabic). https://doi.org/10.21608/jocu.2022.134235.1172

Ahmed, B. S. (2021). The Role of the International Court of Justice in Resolving International Borders Disputes. *Humanitarian and Natural Sciences Journal*, *2*(6), 632–646. (In Arabic).

Akhmatova, D., & Akhmatova, M. (2020). Promoting Digital Humanitarian Action in Protecting Human Rights: Hope or Hype. *Journal of International Humanitarian Action*, *5*, 6. https://doi.org/10.1186/s41018-020-00076-2

Choucri, N., & Clark, D. D. (2013). Who Controls Cyberspace? *Bulletin of the Atomic Scientists*, *69*(5), 21–31. https://doi.org/10.1177/0096340213501370

Cox, L. (2021), *Nationalism: Themes, Theories, and Controversies. Palgrave Macmillan*. https://doi.org/10.1007/978-981-15-9320-8

d'Aspremont, J. (2022). Legal imagination and the thinking of the impossible. *Leiden Journal of International Law*, *35*(4), 1017–1027. https://doi.org/10.1017/s0922156521000637

Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-0320-3

Japaridze, T. (2023). Cyber Sovereignty: Should Cyber Borders Replicate Territorial Borders? In J. Berghofer, A. Futter, C. Häusler, M. Hoell, & J. Nosál (Eds.), *The Implications of Emerging Technologies in the Euro-Atlantic Space* (pp. 209–225). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-24673-9_13

Koulos, Th. (2022). A Digital Territory to be Appropriated: The State and the Nationalization of Cyberspace [version 2; peer review: 2 approved]. *Open Research Europe*, *1*, 119. https://doi.org/10.12688/openreseurope.14010.2

Linden, T., & Shirazi, T. (2023). Markets in Crypto-assets Regulation: Does it Provide Legal Certainty and Increase Adoption of Crypto-assets? *Financial Innovation*, *9*, 22. https://doi.org/10.1186/s40854-022-00432-8

Manshu, Xu, & Chuanying, Lu (2021). China – U.S. Cyber-Crisis Management. *China International Strategy Review*, *3*, 97–114. https://doi.org/10.1007/s42533-021-00079-7

McLean, I., & McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3 ed.). Oxford University Press.

https://doi.org/10.1093/acref/9780199207800.001.0001

Omar, M. O., AlDajani, I. M., Juwaihan, M., & Leiner, M. (2022). Cybersecurity in Sovereignty Reform. In I. M. AlDajani, & M. Leiner (Eds.), *Reconciliation, Heritage and Social Inclusion in the Middle East and North Africa* (pp. 109–128). Springer, Cham. https://doi.org/10.1007/978-3-031-08713-4_8

Osborn, Ph. (2017, October). Cyber Border Security – Defining and Defending a National Cyber Border. *Homeland Security Affairs* 13, Article 5.

Paice, A., & McKeown, S. (2023). Practical Cyber Threat Intelligence in the UK Energy Sector. In C. Onwubiko et al. (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Springer Proceedings in Complexity, Springer, Singapore*. https://doi.org/10.1007/978-981-19-6414-5_1

Pollicino, O. (2020). Metaphors and Judicial Frame: Why Legal Imagination (also) Matters in the Protection of Fundamental Rights in the Digital Age. In B. Petkova, & T. Ojanen (Eds.), *Fundamental Rights Protection Online. Edward Elgar Publishing*. https://doi.org/10.4337/9781788976688.00009

Reiterer, M. (2022). EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacifc. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.). *Cybersecurity Policy in the EU and South Korea from Consultation to Action*. New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2

Sallavaci, O. (2020). Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters. In H. Jahankhani, B. Akhgar, P. Cochrane, & M. Dastbaz (Eds.), *Policing in the Era of AI and Smart Societies, Advanced Sciences and Technologies for Security Applications* (pp 1–58). Springer, Cham. https://doi.org/10.1007/978-3-030-50613-1_1

Segal, A. (2017, June 2). *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Hoover Working Group on National Security, Technology, and Law. Aegis Paper Series, 1703.

Simmons, B., & Hulvey, R. (2023). Cyber Borders: Exercising State Sovereignty Online. *All Faculty Scholarship, 3158*.

Soare, S. R. (2023). Algorithmic power? The Role of Artificial Intelligence in European Strategic Autonomy. In F. Christiano, D. Broeders, F. Delerue, F. Douzet, & A. Géry (Eds.). *Artificial Intelligence and International Conflict in Cyberspace*, Routledge, London. https://doi.org/10.4324/9781003284093-6

St-Hilaire, W. A. (2020). *Digital Risk Governance: Security Strategies for the Public and Private Sectors*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-61386-0

Wang, P. (2022). *Principle of Interest Politics: Logic of Political Life from China's Perspective*. Peking University Press. Springer. https://doi.org/10.1007/978-981-19-3963-1

Zein, M. (2022), The Effect of the New State Sovereignty Concepts on the Jurisdictions of Cybercrime. *International Journal of Doctrine, Judiciary, and Legislation*, *3*(3), 679–738. https://doi.org/10.21608/ijdjl.2022.138565.1159 (In Arabic).

Zekos, G. I. (2022). *Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-94736-1

Zhuk, A. (2023), Virtual Sovereignty: Examining the Legal Status of Micronations in Cyberspace Through the Case of the Republic of Errant Menda Lerenda. *Digital Society*, *2*, 45. https://doi.org/10.1007/s44206-023-00067-x

Сведения об авторе

Абделькарим Яссин Абдалла – судья, суд общей юрисдикции в Луксоре, Министерство юстиции Египта
Адрес: 82516, Египет, г. Сохаг, Мадинат Нассер, ул. Ахмим Сохаг, Нью Касалови Хотел
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.15.41 / Государственный суверенитет
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 21 сентября 2023 г.
Дата одобрения после рецензирования – 12 октября 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.