UDC 341.1/.8:004
Biblid: 0025-8555, 76(2024)
Vol. LXXVI, No. 1, pp. 33–54
DOI: https://doi.org/10.2298/MEDJP2401033S

Review article
Received 13 November 2023
Accepted 17 January 2024


# Cyberspace and Sovereignty in Public International Law

Nikola STANKOVIĆ[1]

**Abstract:** The paper studies the manifestation of cyberspace in the context of the principle of sovereignty as a fundamental principle of public international law. It is a young phenomenon that is still difficult to define in a clear way in the international community. The author analyzes whether, to what extent, and which formal sources of public international law apply to cyberspace. The analysis focuses on three central sources of public international law – international treaties, international customs and general legal rules. Cyberspace is then analyzed from two angles. The first, external aspect of the analysis seeks an answer to the question of whether, first of all, states as central subjects of international public law, but also the international community and to what extent, have sovereignty over cyberspace. Second, internal segment of the analysis is aimed at determining whether cyberspace has its own sovereignty. The paper briefly reviews the perspectives of the leading world powers, above all the United States of America, the People's Republic of China and the Russian Federation. The author concludes that it is necessary to continue working on the regulation of cyberspace, primarily through the institutions of the United Nations. Only regulation at this level can provide the necessary legal regulations that will adequately regulate a specific area such as cyberspace.

**Keywords***:* jurisdiction, state, international community, technology, digitalization, authority.

[1] University of Belgrade – Faculty of Law,
nstankovic@ius.bg.ac.rs, https://orcid.org/0009-0003-4214-7748

## Introduction

Rarely does any branch of law encompass so many social aspects as does the science of public international law with all its complex fragments. By its very essence, and through the sources defined in Article 38 of the Statute of International Court of Justice, it continuously and dynamically reacts to new phenomena in society. New phenomena undoubtedly have an impact on international relations and the international law that regulates them.

One of such phenomena is the initiator for our analysis – cyberspace. This concept rests on a working definition that has been born out of practice (Clark 2010, 1). It is a collection of computing devices that are connected by networks in which electronic information is stored and utilized, but also where communication takes place (Clark 2010, 3). Given that the Internet, i.e. "world wide web" is the key to reaching "digital space", in the introductory part we must define it. The Internet is a vast network that connects computers around the world through which people communicate and exchange information (Britannica). It is a fusion of communication networks, databases and information sources into a global virtual system (Liaropoulos 2013, 21).

Information and individuals are central features to the relevance of cyberspace (Clark, 2010, 3). As we can conclude, we are talking about features that primarily color the definition of the Internet. According to data from April 2022, over five billion people (63.5% of the world's population) use the Internet (Global Era Issues n.d. 2023). By placing both individuals and information in the context of the system of public international law, what we get are two very important segments for that system.

Although he does not have the status of a subject of international law, an individual, understood in a broader sense, is the direct addressee of certain rights and obligations; responsible for the violation of obligations imposed on him by international law (Kreća, 2023, 151-155). Therefore, for individual as an entity of international interest, there is a very important place in the organism of public international law, and consequently a high degree of interest of the international community. This is best evidenced by new developments in the field of international human rights law.

When it comes to information, their relevance is unquestionable. It is enough to expand upon the definition of the international community as a decentralized community composed of states as sovereign political entities that does not know the monopoly of physical coercion embodied in supranational authority (Kreća 2023, 30). In an environment in which the central position belongs occupied to complex

systems such as states, which is decentralized, imbued with a political element and without the apparatus of coercion – information is perhaps a key tool in the adequate normative and political functioning of the international community. The importance of fostering good relations and providing the necessary information is acknowledged through institutions of Diplomatic and Consular Law.

After establishing this connection, the question of the relationship between public international law and the space in which a vast number of individuals spend a lot of time and exchange an unimaginable amount of information opens up. This thesis takes on a completely new dimension when one considers that the majority of states, several important international organizations such as the First Committee of the United Nations General Assembly (GA) on Disarmament and International Security, the G20, the European Union (EU) and numerous others have confirmed that the norms of International law apply to information technology and their use by states (Carnegie Endowment for International Peace 2021). The latest report of the United Nations (UN) open-ended working group from March 2021 also establishes that international law applies to cyberspace, and urges states to avoid or refrain from taking actions that would be inconsistent with positive international law (Heller 2021, 1433). This attitude is a natural consequence caused by the fact that cyberspace is not only a fertile ground for economic progress, but also a space in which a high degree of control and authority can be established – therefore, there is an exceptional interest of actors in international relations to establish regulation over that space via various instruments (Hofmann, Pawlak 2023, 2).

## The relationship between the sources of public international law and cyberspace

Cyberspace is a young phenomenon, which is not even fifty years old yet – it was during the last moments of the twentieth century (Brown, Poellet 2012, 129). Therefore, it is difficult to clearly define which formal sources of Public international law shape this space. The author will analyze three sources that, at least in the literature, are most often discussed – international conventions (treaties), international customary law (customs) and general principles recognized by civilized nations (general principles).

In the context of international contract law, there are still no clear rules governing cyberspace (Carnegie Endowment for International Peace 2021). However, strides have been made in this domain that testify to the opposite, especially in the domain of international criminal law. The author perceives this as

a completely natural sequence of events. Cyberspace is a new phenomenon in every sense, as we have already pointed in the introductory remarks, but it is also a very dangerous one. It is the field for new strategic rivalries and even more dangerous – the ground for the next arms race (Hughes 2010, 523). Since it represents the criminal law of the International Community with the aim of protecting its highest values by applying the most severe criminal sanctions – it is a logical pioneer in this domain (Further: Kreća 2023, 670). The Convention on Cybercrime (Budapest Convention) from 2001 adopted by the Council of Europe is one of the examples of contractual action in the field of cyberspace. Without delving too deeply into the norms of this convention, because that would inevitably take us away from the topic and lead us to the exclusive terrain of International Criminal Law, it is necessary to outline some key guiding ideas of this Convention. Some of them are: appreciation of the drastic changes caused by the digital age and the globalization of computer networks; fear of their use for committing criminal acts and storing evidence in that space; the need to establish interstate cooperation, but also cooperation with the private sector for the purpose of preservation; protection of data, their confidentiality and integrity; establishing the necessary balance between the rule of law and respect for human rights, as established primarily by the European Convention on Human Rights, The International Covenant on Civil and Political Rights, but also by other relevant instruments in the field of human rights protection... (CE [2010] European Treaty Series – No. 185)

In a more recent time frame, more precisely in 2019, the UN General Assembly voted to start the process of negotiations on the adoption of the Convention on Cybercrime by adopting the Resolution on countering the use of information and communications technologies for criminal purposes, which would expand this issue on the global stage (UN Regional Information Centre for Western Europe n.d.). Also, an ad hoc committee was established with the task of dealing with this issue in the future (UN Regional Information Centre for Western Europe n.d.). It is interesting that at the The Internet Governance Forum in 2019, among others, former Chancellor of Germany Angela Merkel said: „We need to agree on how to protect human rights, democracy and the rule of law in the digital age, how to strengthen equal participation and security online and how to build trust in her“ (UN Regional Information Centre for Western Europe n.d.).

In the second place, there are rules International Customary law. Customary rules are at the heart of International Law (Milisavljević 2016, 7). A rule of Customary International law is comprised from two elements: practice and sense of legal obligation (Kreća 2023, 113). The element of practice is slowly starting to appear in international relations (Brown, Poellet 2012, 129). *Opinio juris* is a

qualitative element of custom and a qualifying condition that turns practice into common law (Kreća 2023, 115). It's already more difficult establishment due to its subjective nature is in this domain reinforced by the secrecy of cyber operations (Brown, Poellet 2012, 129). The very nature of the modern international legal order contributes to the favorable ground for preserving the secrecy of state operations in cyberspace. Namely, there is no international body that states can turn to in order to collect evidence and carry out the procedure to determine the intent behind the state's practices in cyberspace (Brown, Poellet 2012, 136). Even if some evidence is clearly established, the state in question can easily resort to labeling that data as secret, especially since it can be politically sensitive (Brown, Poellet 2012, 136). In the same context, states that are victims of cyber-attacks will not want to publicly admit it to the entire international community (Brown, Poellet 2012, 136). Therefore, we can conclude that the role of International Customary Law in this domain is still in the development phase (Brown, Poellet 2012, 141).

Practice, however, mostly relies on principles embodied in general principles recognized by civilized nations, more precisely the security segment of this space (Shao 2021, 90). For example, the policy of the United States of America (USA) in this sense is indisputable because the USA has taken the position in its foreign policy that the established principles of international law apply to cyberspace as well (Koh 2012, 3). These principles, although they are not on the pedestal that they rightfully belong to in International customary and treaty law, produce legal consequences and create a normative space for the genesis of precise legal norms precisely within the framework of these two sources (Further: Tsagourias 2021, 19). The author believes that the legal *status quo* is „a medal with two faces". Namely, it enables the flexibility of the international legal order, which is necessary so that this phenomenon could be kept within the framework of the international legal order in the broadest sense, but on the other hand, it is necessary for the principles to be a „passing point" on the way to a more precise and clear regulation, as only customs, and especially international treaties can provide. We must not lose sight of the fact that general legal principles are the most controversial source of Public international law, on which, since the adoption of the Statute of the Permanent Court of International Justice, no clear consensus has been reached either in terms of nature, scope or role – however important and affirmed that role may be in modern International Law (Shao 2021).

## The interplay between cyberspace and sovereignty: public international law perspective

After affirming the international legal order as the current and, more importantly, the future regulator of cyberspace on the international level, we can address the issue debated by numerous recognized authors in the international community – the relationship between cyberspace and the principle of sovereignty. In order to open the issue of the mentioned relationship in general, it is necessary to start from the concept of sovereignty and how it is understood in the legal discourse (Tsagourias 2021, 17).

The state as a key subject of international public law is cumulatively determined by three elements: steady population; established territory; sovereign power (Kreća 2023, 158). Sovereignty is considered a qualifying condition of a special rank (Kreća 2023, 159). It is a fundamental principle of international law (Tsagourias 2021, 16). The Permanent Court of Arbitration provided a definition of sovereignty in the Las Palmas case (Heller 2021, 5). Without going into the Court decision itself, the concept of sovereignty has an internal and an external dimension (Heller 2021, 5). The internal dimension includes the territorial (the right of the state to establish supreme authority over all persons and objects within its territory without the influence of other states) and the state type (the right to choice of its political, economic, social and cultural model of organization) (Heller 2021, 5). The external dimension implies the equality of all states under the umbrella of International Law, having the same rights and being bound by the same obligations towards the international legal order (Heller 2021, 5).

While the internal dimension is indisputable, the external one is rather relativized (Tsagourias 2021, 17). She reaches out to the international legal system (Liaropoulos 2013, 22). The principle of sovereign equality of member states of the international community automatically imposes a limitation of sovereignty precisely at the point where they touch each other (Further: Tsagourias 2021, 17). In order for this touching not to grow into encroachment, subjugation, swallowing – it is necessary to reach a consensus between the states that which will guide this system on external plane (Further: Tsagourias 2021, 17). Some authors define this duality also as territorial sovereignty on the internal level, and state integrity on the international level (Pirker 2013, 191). Furthermore, it is very important to separate territory from sovereignty as such, regardless of the clear territorial element present. Namely, the territory is a component of the principle of sovereignty (Tsagourias 2021, 17). It is the outcome of the political process of the organization of space in the international community which involves claims,

counterclaims and assertions of power (successful ones) (Tsagourias 2021, 18). At the heart of this principle is power, not territory (Tsagourias 2021, 18). Another institute of International law derives from it, which we must refer to briefly – the jurisdiction of states. The principle of sovereignty is operationalized through this institute (Tsagourias 2021, 19). It is the power of the state to regulate or otherwise influence individuals, property and circumstances within the framework of international law, but it is also a vital feature of state sovereignty (Pirker 2013, 196).

The relevant principles for determining jurisdiction, which derive from criminal law, are: the territorial principle, the principle of nationality, the protective principle, principle of universality, passive national principle (Kreća 2023, 232-233). The most important forms of jurisdiction are territorial jurisdiction, which includes the jurisdiction of the state authorities of a country over all things and persons located on its territory; extraterritorial jurisdiction directed at the same objects, but outside the state territory; strictly internal jurisdiction, which includes the area in which the state sovereignly and independently of international law regulates relevant relations, and international jurisdiction, which includes matters in which the international community holds jurrisdiction (Kreća 2023, 234-238).

The relationship between the principle of sovereignty and cyberspace, prima facie presents different problems, which can all be reduced, according to the author's opinion, to one common problem – the problem of determining clear boundaries of different sovereignties in such a globalized digital space. For example, cyber attacks cross national borders and are difficult to trace, but they also affect military and civilian networks (Liaropoulos 2013, 19). However, the most diverse activities in cyberspace can encroach on all elements of society, both internally and internationally, not only in terms of cyber attacks, nor only directed at the military and civilian networks of a country.

Conceptually, cyberspace is in deep conflict with the principle of sovereignty. Namely, it was created as a completely open space that has connection instruments that are completely independent of the state and its authority (Adams, Albakajai, 2016, 257). This very step is interpreted by some as a violation of state sovereignty (Adams, Albakajai, 2016, 257). Then, cyberspace is itself a non-territorial domain (Liaropoulos 2013, 21). In various places in the literature, the author finds that this is one of the key factors in the problem of regulation of cyberspace because, on the one hand, it is not bound by borders in the classical sense, and on the other, in a related sense – that is why it is difficult to determine where an activity originates from. In contrast, international legal sovereignty is colored to a significant extent by the territorial component (Tsagourias 2021, 17). It follows from this that states have an obvious interest in overcoming this feature of cyberspace and establishing the principle of sovereignty in cyberspace as well (Liaropoulos 2013, 22).

In this sense, the work will be based on the methodological approach proposed by Nicholas Tsagourias, which is based on finding answers to two questions: whether cyberspace can be subject to the principle of sovereignty and whether cyberspace itself can be sovereign (Tsagourias 2021, 16).

The state has jurisdiction over the infrastructure necessary for the functioning of cyberspace located on its territory (Tsagourias 2021, 19). The owner of that infrastructure is either government or private corporation within its territory, and it is connected to state's electric grid (Heintschel von Heinegg 2013, 126). Without it, cyberspace itself could not exist. This infrastructure, by the very fact that it is located in real space, is subject to state sovereignty (Liaropoulos 2013, 22). A factor that the author perceives as underestimated, especially by supporters of cyberspace is immune from state sovereignty, is that it cannot function in „chaos" but requires regulation and supervision (Liaropoulos 2013, 22).

The state can also impose technical restrictions on that infrastructure through, for example, imposing entry passwords (Tsagourias 2021, 21). Jurisdiction extends to citizens, but also to foreigners who are in the territory of the respective state and who engage in cyber activities (Tsagourias 2021, 19). Also, informations that flow through cyberspace are subject to the jurisdiction of the respective state both at the point of delivery, but also at the point of reception (Tsagourias 2021, 19). The same applies to the wires and lines used in that process – they are within the jurisdiction of the state in whose territory they are located (Tsagourias 2021, 19).

However, territoriality and nationality, as the bases of jurisdiction can be subject to a very broad interpretation and expand even further the scope of a state's jurisdiction and thus sovereignty (Tsagourias 2021, 19). In essence, it is about the implementation of extraterritorial jurisdiction over citizens who participate in cyber activities outside the territory of the respective state, but obviously not outside its jurisdiction, its sovereignty(Further: Tsagourias 2021, 19). However, this is not an easy task at all. Namely, the principles of establishing jurisdiction can be applied simultaneously and thus their content may be subject to different interpretations, overlaps and even confliction (Pirker 2013, 197). The above-mentioned rule also applies if the citizen is the victim of some cyber activity in the specific case (Tsagourias 2021, 19). Moreover, on the international level, a consensus has been reached that a certain cyber activity may constitute a violation of the principle of prohibition of the threat or use of force, and authorize the state to resort to the right of self-defense (Heller 2021, 1).

A very interesting aspect of this debate is also the right of the state to establish its jurisdiction and subject to its own sovereignty the cyber activity that has effects in its respective territory (Tsagourias 2021, 20).

However, although it is a doctrine that was confirmed in the Lotus case by the Permanent Court of International Justice – it is very difficult to apply it in the context of cyberspace since it concerns activities that easily affect reached a number of different jurisdictions (Tsagourias 2021, 20). Quite naturally, different states then have an interest in establishing jurisdiction over a specific activity – and a collision of different sovereignties arises (Tsagourias 2021, 20). In order to avoid collision, the standard from certain minimum contacts has been risen to substantial contacts (Tsagourias 2021, 20). Moreover, a country that is the target of a cyber-attack or some other operation can take adequate countermeasures against the country that carried out that activity (Heller 2021, 4). The state must be present in cyberspace and exercise control also in order to preserve its national interest (Liaropoulos 2013, 22). Cases of endangerment of the national interest mainly concern the suspicion that espionage has been carried out against a state through cyberspace (Tsagourias 2021, 20). In this sense, states are determined and continuously emphasize that they have the right to exercise jurisdiction over cyber structures and activities, in order to protect themselves from foreign interference by other states or individuals (Heintschel von Heinegg 2013, 126).

The author, however, believes that this is a very dangerous terrain. Due to their consensual nature, international law and international relations are burdened with a political element, yet they are forced to communicate within the framework of the international community, which has become highly interdependent. Therefore, the exceptional importance of the instruments of diplomatic and consular law, although contribute to shaping the national interest and the perception of its violation – in the context of a space such as cyberspace, the political dimension and its abuses grow exponentially.

In addition to such direct pretensions to subjugate cyberspace, there are also indirect ones. Namely, submitting to sovereignty also exists in cases of limiting access to certain Internet content and cyber activities within one's territory (Tsagourias 2021, 20).

Usual examples of this limitation are People's Republic of China and North Korea. At the same time, just as a state can limit cyber activities, the exercise of its sovereignty can be limited by customary and treaty norms of International law, such as the protection of diplomatic correspondence, the right of free navigation and transit (Heintschel von Heinegg 2013, 128). The protection of the diplomatic staff and diplomatic premises should be added to these same restrictions, as well as the regulation of Internet access in accordance with International human rights law, as well as telecommunications law (Pirker 2013, 192).

Continuing our analysis, we arrive at the answer to the question why it was so important to clearly mention that territoriality, although important, is only one element of the principle of sovereignty. As we said, the essence lies in effective authority, effective government. In this context, states have the possibility to establish jurisdiction, either unilaterally or jointly with other states, over objects and activities in cyberspace because they, at least originally, do not fall under anyone's jurisdiction (Tsagourias 2021, 20). The legal connection with the real world, as we have already mentioned, is reflected in the regulation and jurisdiction over cyber infrastructure. In addition to this "legal" argument, the factual argument also lies in the fact that cyber activities can have a significant impact on the real space, therefore also the states that sovereignly rule that space (Further: Liaropoulos 2013, 22).

Here again, in a very interesting way, the feature of „territorial" comes to the fore. Namely, that feature has almost spilled over into cyberspace and affects its territorialization in the sense of establishing authority and penetration of sovereignty into a space that is inherently devoid of such influence, and on the other hand, that spillover only reinforces the idea of the existence of sovereignty beyond traditional concepts (Further: Tsagourias 2021, 21).

The analysis of the first segment is thus concluded, and now we can move on to the question of the (non)existence independent cyberspace sovereignty. We have already said that cyberspace is a territorial space in itself, and the trend of separating the concept of sovereignty from territory as such will inevitably continue. However, it is obvious, already from the terminology itself, that cyberspace is some kind of space.

That space certainly cannot be physically measured since it defies measurement in any physical dimension or time space continuum (Heintschel von Heinegg 2013, 125). Therefore, we must not look at the territory through the usual geographical prism, but as a social construct, a perception (Tsagourias 2021, 22). Perceived in that way, cyberspace can be described as as a figurative or noumental space inhabited and experienced through machines by people who are located in real spaces (Tsagourias 2021, 22).

Viewed in this way, cyberspace and its own sovereignty inevitably acquire a practical importance, not just a theoretical one. As technology advances, becomes more accessible and the content within cyberspace becomes more connected to people's everyday life, this issue will inevitably come before the internal, but especially the international legal order.

The analysis of this aspect of cyberspace sovereignty is incomplete without reference to the so-called „Declaration of the Independence of Cyberspace". This

is a libertarian idea that was advocated by John Perry Barlow when he published this text in 1996 in Davos (Wired n.d. 2023). This text is full of truly utopian ideas. Barlow calls on states as „ghosts of the past" not to enter cyberspace because they are neither welcome nor have sovereignty there (Electronic Frontier Foundation n.d. 2023). Furthermore, he points out that there is no moral right to establish such sovereignty, but also that, on the other hand, there are no methods of enforcement that generate true fear (Electronic Frontier Foundation n.d. 2023).

It is interesting that he also, in a way, refers to the principle of consensualism because he points out that the modern system of government requires the consent of those who are the bearers of power, that is, in the international legal context – the bearers of sovereignty (Electronic Frontier Foundation n.d. 2023). Since there is no consent of cyberspace users, there can be no question of imposing someone else's sovereignty (Electronic Frontier Foundation n.d. 2023). He continues, pointing out that cyberspace rests on a separate and specific social contract that will give birth to its own power, thus its own sovereignty (Electronic Frontier Foundation n.d. 2023). He points out that cyberspace is everywhere, but also nowhere (Electronic Frontier Foundation n.d. 2023).

He points out that in cyberspace any intellectual creation can be created free of charge and then distributed infinitely (Electronic Frontier Foundation n.d. 2023). Barlow concludes that cyberspace will inevitably spread across the globe, therefore fleeing from national sovereignty (Electronic Frontier Foundation n.d. 2023). Although hardly anyone went this far, there were authors who believed that the only adequate solution was the formation of a special Internet law that would regulate cyberspace (Pirker 2013, 193). Certainly, the author perceives this text more as a curiosity when it comes to understanding of the cyberspace by a certain part of its users, that is at best a mere imagination because it completely ignores the normative and political realities of the modern international community.

Any equating of internet users in cyberspace with the nation as the bearer of sovereignty, which would then express its will for the formation of a separate entity through the right to self-determination – is unrealistic according to the author. At the heart of this principle lies the idea that nation has the right to decide on their own internal establishment as well as representation on the external plane – as we said, we take the position that this group of users cannot be labeled as a nation (Tsagourias 2021, 23).

Without going into the issue of defining nation as the most important group – even if we recognize such a status for users of cyberspace, the right to self-determination is already problematic and fertile ground for political abuses in actual practice. It is not an absolute right because, as such, it would lead to chaos

and anarchy in the international community (Kreća 2023, 637). Without going deeper into the idea of „cyber nation", the author will only highlight the following, obvious fact. No matter how widespread and intensified the use of cyberspace is, its participants did not, by entering the digital space, lose the real civic connection with the country they come from, which inevitably entails a series of rights, but also obligations, and is an indisputable extension of the sovereignty that their country has over them. Any decision to proclaim the sovereignty of cyberspace will be subject to the scrutiny of their own State (Tsagourias 2021, 24). Even if such a decision were to be made, the normative and institutional instruments necessary for its maintenance do not exist or, paradoxically, would depend on the very states from whose sovereignty they are trying to escape (Tsagourias 2021, 24). Therefore, we can conclude that cyberspace can be subject to sovereignty, but it does not have its own (Tsagourias 2021, 24). The author adds here that this space is already within the sovereignty of different states.

Completing this analysis requires us to look briefly at the aspect of cyberspace as a common good of the entire international community. Truth be told, it seems logical to place the space that is colored by anonymity and ubiquity in the same group as the open sea, space and air space (Heintschel von Heinegg 2013, 125). If cyberspace were to be perceived like this, it would cause several significant consequences. Primarily, any state with the appropriate technical means would be enabled to access and exploitation of cyberspace (Tsagourias 2021, 25). Then, the question of the jurisdiction of the international community over this space would be opened – bringing us back to the principle of sovereignty (Tsagourias 2021, 25). The idea of classifying cyberspace as a common good of all humanity – has not reached a relevant level of consensus in the international community (Pirker 2013, 194). Therefore, we will not deepen our analysis here.

## The perspective of World Powers

Modern international community is, more than ever before, imbued with interdependence and interconnection. In such environment, most influent community members affect its functioning greatly. Question of sovereignty in cyberspace is no exception. In the interest of temperance, author will focus his analysis on brief review of stances by the Russian Federation (Russia), People's Republic of China (China) and finally United States of America (USA).

Russian authorities perceive cyberspace as "territory with virtual borders corresponding to physical state borders, and wishes to see the remit of

international laws extended to the internet space, thereby reaffirming the principles of sovereignty and non-intervention" (Asmolov and Kolozaridi 2020, 279). It classifies it under a broader category of "information space" or "information enviroment" which includes all mass media (Nikkarila and Ristolainen 2017, 2). Back in 2016, NATO declared that cyberspace represents a military domain (Nikkarila and Ristolainen 2017, 2). During the same year Russian president Vladimir Putin signed the Information Security Doctrine with aim to deploy a national system of managing the Russian segment of the Internet (Nikkarila and Ristolainen 2017, 2). "RuNet" – Russian segment of the internet was to be disconnected from the global internet by 2020 (Nikkarila and Ristolainen 2017, 2). Russian perception is that internet is a product of American coulture, and thus free information flow proposes a threat to Russian cultural integrity and independence (Nikkarila and Ristolainen 2017, 2). If state controls the internet, (and thus cyberspace), its defence against external attacks grows stronger (Nikkarila and Ristolainen 2017, 2). Next year, in 2017, Russia took further steps in direction of establishing clear and dominant sovereignty in cyberspace. Two legislations were signed into law, law Law № 276-FZ and 241-FZ (Human rights watch 2017). First law denies owners of virtual private network also known as VPN services and internet anonymizers to provide acces to websites banned in Russia (Human rights watch 2017). Russia's federal executive authority "Roskomnadzor" is authorized and responsible for overseeing online and media content, but also to block sites that provide instructions on bypassing the government blockage (Human rights watch 2017). Also, creating a registry of online resources and services prohibited in Russia is a task for "Roskomnadzor" and law enforcement agencies have the authorization to identify violators (Human rights watch 2017). When it comes to the second law, it prohibits access to online messaging applications to unidentified users considering access that could be provided by companies registered in Russia as "organizers of information dissemination" (Human rights watch 2017). Mobile applications that fail to comply with requirements to restrict anonymous accounts will be blocked in Russia (Human rights watch 2017).

Project "RuNet 2020" aims at "digital sovereignty" (Nikkarila and Ristolainen 2017, 2). On the path for complete national governance over internet in Russia, in 2019 "Sovereign internet" legislation passed (SecAlliance 2018). It allowed "Roskomnadzor" to take control of network in case of national emergency and puts a time frame for implementation of national domain space for January 2021 (SecAlliance 2018). During 2019 Russia successfully tested a country wide alternative to global internet (BBC 2019). However, as of 2023, testing is still underway and it had it ups and downs. For instance, when Russian government tried to block twitter (now "X", remark by author) in 2021, it also blocked Kremlin

websites (Scientific American 2023). Without delving into complex and relevant aspects of such activities violating human rights, regarding the topic of this article, it is obvious that there are clear political and legal steps being taken by Russian government in order to extend its sovereignty into Cyberspace.

When it comes to China, The Chinese Communist Party has taken steps to control internal and external flow of information both domestically and internationally (JSTOR 2019). It, as Russia, perceives cyberspace as part of "information domain" control over which it finds critical for future great-power conflict (JSTOR 2019). Already, we have a clear political signal that China has immense interest of establishing state sovereignty in this domain, including cyberspace. Cyber policy in China is developed and implemented within, national policy system called xitong (Attril and Fritz 2021, 3).

Significant online content filtering system known as the Great Firewall dates 20 years back (Peixi 2021, 3). In 2015, Chinese president Xi Jinping proposed the notion of cyber sovereignty as a response to external cyber threats (Peixi 2021, 3). Also, same year is marked by the launch of the Great Canon which has the ability to alter and replace content as it traverses the Internet (ICS 2023). This is very important since it modifies unobscured access to Cyberspace, and perception of it by the Chinese user base. Unlike in the case of Russia, China does not seek to create its own alternative version of internet but to harness the transformative power of cyberspace for its own interests (Attril and Fritz 2021, 9).

On the other hand, economic potential within Cyberspace, which was in 2020 estimated be worth around 6 billion United States dollars, also plays significant part in motivating China to get a grasp over this space and support many developing cyber norms proposed by both state and non-state actors (Peixi 2021, 4). Author finds this to be a significant difference when compared to previous example of Russia where economic aspect due to geo-political factors is not as strong. Virtual private networks underwent a serious crackdown ordered by Xi Jinping personally (ICS 2023). China seeks to develop in a "Cyber superpower" (Attril and Fritz 2021, 3)

In 2015, Chinese State Council promulgated an "Internet Plus" document that promoted deep integration of the internet with all the aspects of China's economy and society (Lee 2022, 10). Same author provides an interesting fact. Namely, in the same year that president Jinping came into power, it was disclosed in the Snowden leaks that Chinese cybersecurity is quite compromised, mainly by USA (Lee 2022, 11). This resulted in creation of Central Commission for Cybersecurity and Informatization (CCCI) with Cyberspace administration of China (CAC) acting as executive office (Lee 2022, 11). Late 2010's where marked by releases of many

draft laws and policies concerning cyberspace for public consultation (Lee 2022, 12). In 2016, China Introduced its national Cybersecurity Law (Lee 2022, 12). China continued with this trend and during 2021 and 2022 adopted Data Security Law (DSL), Personal Information Law (PIPL), Five Year Plan for National Informatization (FYPNI), and other regulations aimed at regulating commercial activities in Cyberspace (Lee 2022, 14). After 2018 CAC was placed under the authority of Central Cyberspace Affairs Commission which made its authority and overall responsibilities clearer (Attril and Fritz 2021, 4). These efforts (both legislative and political) resulted in clear policy guidelines for state intervention in Cyberspace and generating a comprehensive institutional system and regulatory framework (Lee 2022, 14). CSL, DSL and PIPL are pillars of modern Chinese Cyberspace regulation (Lee 2022, 22). Xi Jinping argues that states have the right of choice when it comes to path of cyber development, model of cyber regulation, and internet public policies, and participate in international cyberspace governance on an equal footing (Attril and Fritz 2021, 9). Thus, there is no dilemma that China seeks to empower its sovereignty over new, digital landscape of the future. Even the Cyber Administration of China published an academic paper which explicitly states that cyber sovereignty is a natural extension of state sovereignty in cyberspace (Attril and Fritz 2021, 10).

Final reflection takes us on the other side of the world, key representative of modern liberal society – United States of America. USA invests heavily into internet technologies (65$ billion dollars), and president Biden's administration claims that securing Cyberspace is essential for realizing all the benefits of potential digital future (White House D.C. 2023, introduction). This goes for both private and public sectors (White House D.C. 2023, introduction). Further, it insists on strengthening norms regulating state behavior in cyberspace (White House D.C. 2023, 2). USA seeks to create resilient, defensible digital ecosystem aligned with its own values (White House D.C. 2023, 1). It is interesting to note, that even though USA approaches Cyberspace in a more liberal way than previously mentioned states in this segment, it also states that it has interests in this domain (White House D.C. 2023, 3). It also states that Russia and China, among other autocratic regimes as perceived by the White House act in Cyberspace with disregard for rule of law and human rights which threatens USA national interests and economic prosperity (White House D.C. 2023, 3). This is quite dangerous and only further testifies about ever-present state sovereignty in Cyberspace.

It is very important to mention the Office of the National Cyber Director (ONCD) which advises the President of the United States on cybersecurity and policy (White House). It is a part of Executive office of the President (White House). Its mission is to advance national security, economic prosperity, and technological innovation

through cybersecurity policy leadership (White House). In this sense it is also important to take notice of U.S. Department of Homeland Security. This department proclaims Cyberspace as most active threat domain in the world and most dynamic threat to Homeland (Homeland Security). It emphasizes the significance of critical infrastructure in sense that nation-states are targeting it to gather both information and access to industrial control systems in the energy, nuclear, water, aviation, and critical manufacturing sectors (Homeland Security). This organically corresponds with what was stated earlier in the article considering connection between infrastructure and Cyberspace, opening doors for sovereignty in this arena. A component of the Department of Homeland Security is also Cybersecurity and Infrastructure Security Agency ("CISA") – the federal agency responsible for protecting critical infrastructure in the United States (ICLG 2023). Department of Homeland security focuses on four goals: Secure Federal Civilian Networks, Strengthen the Security and Resilience of Critical Infrastructure, Asses and Counter Evolving Cybersecurity Risks and combat Cybercrime (Homeland Security).

From the turn of the century, US normative building was quite active when it comes to cyber activities and consequently cyberspace. We will mention some relevant norms. Considering cybercrime, some of relevant federal laws are The federal Computer Fraud and Abuse Act ("CFAA") and Electronic Communications Protection Act (ECPA) (ICLG 2023). When taking into account cybersecurity particularly relevant is The Federal Trade Commission ("FTC") and Cybersecurity and Infrastructure Security Agency Act (ICLG 2023). In 2022, president Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) (ICLG 2023). There are also numerous state and sector rules and regulations, which due to excessive quantity, we will not be analyzing here. A common denominator for part of cyberspace regulation is the interest of protecting minors online. This common thread is found in Communications Decency (CDA) Act from 1996, Internet Online Summit from the following year, Children Online Protection Act (COPA) from 1998 and Children Internet Protection Act (CIPA) from the turn of the millennium (Ignou 11).

Finally, USA National Cyber Security strategy from 2023 states that USA used multilateral processes like the United Nations (UN) Group of Governmental Experts, Open-Ended Working Group in order to develop a framework which includes peacetime norms and confidence-building measures, affirmed by all UN member states in the UN General Assembly (White House). It also advocates for expanding the Budapest Convention on Cybercrime and making other efforts to make Cyberspace a more secure domain (White House). Further, it reaffirms its support for applicability of International Law and further diplomatic action in order to create a stable cyberspace and condemn state behavior within it (White House).

To conclude this segment, it is apparent that mentioned world powers have clear political and legislative interests to affirm their sovereign presence in Cyberspace, from a national perspective. Russia's intention to basically create separate national Cyberspace and China's to induce control over every single information passing through its portion of Cyberspace negatively impacts further normative work of the United Nations since it clearly demonstrates lack of interest by these States to approach Cyberspace from a uniform, global perspective. Even though USA is neither so extreme, or restrictive, it is clear that it has its national interests in Cyberspace which it regulates from a national perspective. Even though it proclaims endorsement of UN mechanisms and approach, it is very important to note that that endorsement is in function of bringing closer other States to its own value system. Bearing in mind the complexity of international community in both cultural, historical, social, legal and political sense – this also has a rather relevant negative potential for uniform action through UN institutions.

## Conclusion

The question of the relationship between cyberspace and sovereignty is the embodiment of the aspiration of modern public international law to provide answers to new phenomena in global society. Cyberspace as a specific, new, territorial „place" of gathering for a huge number of the world's population is no exception. It produces consequences in the real world and the modern international community, as well as its members, have a high degree of interest in adequately addressing this issue.

However new the phenomenon may be, we pointed out that it is certainly covered by the system of public international law, although primarily through general legal rules recognized by civilized nations. Author stands on the position that practice and then customs will definitely be created in this domain, as well as that international treaty law will not lag behind in the process of clearer regulating of cyberspace. This is evidenced by the clear political and legal efforts of the states, but also of the United Nations.

At the same time, it is very important to understand the flexibility provided by the system of International law in a responsible way and to continue working on the directing from general principles as source references towards true pillars of the science of Public international law represented by international treaties and customary rules. For now, in this sense, international criminal law is leading the

way as a fragment of public international law, as we have shown by referring to the Budapest Convention.

In terms of answering the question of the relationship of sovereignty and cyberspace, two very important questions were raised. For their answer to be complete, it was necessary to highlight both the principle of sovereignty and the institute of jurisdiction as a form of its institutionalization. Of imperative importance is the separation of the principle of sovereignty from territory as its important component. Let us recall that the essence of the principle of sovereignty is effective power, not territory as such. This is the only way we can approach the specific territorial creation and the activities that take place within cyberspace.

As far as the first question is concerned, we pointed out that there is no doubt that the state justifiably has interest and jurisdiction over cyberspace. The most plastic evidence of this is the territorial attachment of the cyber structure to the territorial sovereignty of the country within which it is placed. A more politically dangerous, but also very important segment of the subject analysis is the preservation of the national interest of states and protection from cyber-attacks. Therefore, it is indisputable that the sovereignties of states can be linked to cyberspace and that it is subject to them.

When it comes to the second issue, we have seen that libertarian approaches like the one advocated by Barlow in the „Declaration of Independence of Cyberspace" are fictions rather than attitudes that appreciate the pervasive political, legal, and real circumstances of the modern interdependent international community. The users of this space remain tied to their countries by citizenship ties and do not create any „cyber nation" that could then rely on the already problematic right to self-determination. Although meaningful, the categorization of cyberspace as a common good – is not even close to the necessary consensus to be placed in the same family as the regulation of, say, the open sea and the cosmos.

We also saw that the matter of sovereignty in cyberspace has also quite practical aspect when we briefly analyzed cases of Russia, China and USA. It is clear that not only do states, primarily first two, have interest to establish sovereignty in Cyberspace, but that they also tend to monopolize it. Even though USA is, expectedly much more liberal in this sense, one cannot deny its national interests in cyberspace, both domestically and internationally.

The author believes that there must be further, more intensive work by the UN here, which will produce the necessary resolutions in this domain in the near future. This is the only way to achieve adequate regulation of a specific space such as cyberspace, which respects the interests of cyberspace users, member states, but also the international community to which they belong.

## References

Adams, Jackson and Mohamad Albakajai. 2016. "Cyberspace: A New Threat to the Sovereignty of the State". *Management Studies* 4 (6): 256-265.

Asmolov, Gregory and Polina Kolozaridi. 2020. "Run Runet Runaway: The Transformation of the Russian Internet as a Cultural-Historical Object". *The Palgrave Handbook of Digital Russia Studies* (chapter 16): 277-296.

Attril, Nathan and Audrey Fritz. 2023. China's cyber vision: How the Cyberspace Administration of China is building a new consensus on global internet governance. *International Cyber Policy Centre Policy Brief Report No. 52/2021.*

BBC. 2019. Russia 'successfully tests' its unplugged internet. https://www.bbc.com/news/technology-50902496.

Brown, Gary and Keira Poellet. 2012. "The Customary International Law of Cyberspace". *Strategic Studies Quarterly* 6 (3): 126-145.

Carnegie Endowment for International Peace. 2021. n.d. "A Brief Primer on International Law and Cyberspace". Accessed 5 September 2023. https://carnegieendowment.org/files/Hollis_Law_and_Cyberspace.pdf.

Computer Science and Artificial Intelligence Laboratory Massachusetts Institute of Technology. 2010. n.d. "Characterizing Cyberspace: Past, Present and Future". Accessed 7 September 2023. https://dspace.mit.edu/bitstream/handle/1721.1/141692/Clark%20%282010%29%20Characterizing%20cyberspace.pdf?sequence=1&isAllowed=y.

Council of Europe. 2001. Convention on Cybercrime. European Treaty Series – No. 185, November 23. https://rm.coe.int/1680081561.

Electronic Frontier Foundation. "A Declaration of the Independence of Cyberspace". Accessed 9 September 2023. https://www.eff.org/cyberspace-independence.

Heintschel von Heinegg, Wolff. 2013. "Territorial Sovereignty and Neutrality in Cyberspace". *International Law Studies* 89 (123): 123-156.

Heller**,** Kevin Jon. 2021. "In Defense of Pure Sovereignty in Cyberspace". *Forthcoming, International Law Studies* 97 (1432): 1433-1499.

Hongju Koh, Harold. 2012. "International Law in Cyberspace". *Harvard International Law Journal* 54: 1-12.

Hughes, Rex. 2010. "A treaty for cyberspace", *International Affairs* 86 (2): 523-541.

Human Rights Watch. 2017. Russia: New Legislation Attacks Internet Anonymity. https://www.hrw.org/news/2017/08/01/russia-new-legislation-attacks-internet-anonymity

ICLG.2023. Cybersecurity Laws and Regulations USA. Accessed 16.01.2024. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa

ICS Research blog. 2023. Internet Censorship in China: The Struggle to Swat "Flies" Away. https://icsin.org/blogs/2023/10/10/internet-censorship-in-china-the-struggle-to-swat-flies-away-2/

Ignou University. The Regulability of Cyberspace. Accessed 15.01.2024. https://egyankosh.ac.in/bitstream/123456789/7531/1/Unit-10.pdf

JSTOR. 2019. Are China and Russia on the Cyber Offensive in Latin America and the Caribbean?. https://www.jstor.org/stable/resrep19975.4

Kreća, Milenko. 2023. *Међународно јавно право*. Beograd: Univerzitet u Beogradu – Pravni fakultet.

Lee, John. 2022. "Cyberspace Governance in China: Evolution, Features and Future Trends", *Asie.Visions, No. 129*

Liaropoulos, Andrew. 2013. "Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?". *Journal of Information Warfare* 12 (2): 19-26.

Milisavljević, Bojan. 2016. *Међународно обичајно право*, Beograd: Univerzitet u Beogradu – Pravni fakultet.

Nikkarila, Juha-Peka and Mari Ristolainen. 2017. "'RuNet 2020' – deploying traditional elements of combat power in cyberspace?". Paper presented at International Conference on Military Communications and Information Systems (ICMCIS).

Peixi, Xu. 2021. "A Chinese Perspective on the Future of Cyberspace", *Cyberstability Paper Series New Conditions and Constellations in Cyber*.

Pirker, Benedikt. 2013. "Territorial Soveregeinty and Integrity and the Challenges of Cyberspace". In: *Peacetime Regime for State Activities in Cyberspace,* edited by Katharina Ziolkowski, 189-214. Tallinn: NATO CCD COE Publication.

Regional Information Centre for Western Europe. 2022. "A UN treaty on cybercrime en route". United Nations. Accessed 9 September 2023. https://unric.org/en/a-un-treaty-on-cybercrime-en-route/.

Scientific American. 2023. Russia Is Trying to Leave the Internet and Build Its Own. https://www.scientificamerican.com/article/russia-is-trying-to-leave-the-internet-and-build-its-own/

SecAlliance. 2018. Digital sovereignty in the age of connectivity: RuNet 2020. https://www.secalliance.com/blog/runet-2020

Shao, Xuan. 2021. “What We Talk about WhenWe Talk about General Principles of Law”. *Chinese JIL*. DOI: https://doi.org/10.1093/chinesejil/jmab019.

Taylor and Francis Online. 2022. “Governing cyberspace: policy boundary politics across organizations”. Routledge. Accessed 8 September 2023. https://www.tandfonline.com/doi/full/10.1080/09692290.2023.2249002?scroll=top&needAccess=true&role=tab .

The White House. 2023. National Cybersecurity Strategy. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The White House. Office of the National Cyber Director. Accessed 15.01.2024. https://www.whitehouse.gov/oncd/

Tsagourias, Nicholas. 2021. “The legal status of cyberspace: sovereignty redux?”. *Research Handbook on International Law and Cyberspace*. DOI: https://doi.org/10.4337/9781789904253.00010.

U.S. Department of Homeland Security. Secure Cyberspace and Critical Infrastructure. Accessed 15.01.2024 https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure

Wired. 2016. “It’s Been 20 Years Since This Man Declared Cyberspace Independence”. Accessed 9 September 2023. https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/.

World 101. 2023. “The Internet By Numbers”. Global Era Issues. Accessed 7 September 2023. https://world101.cfr.org/global-era-issues/cyberspace-and-cybersecurity/internet-numbers#:~:text=As%20of%20April%202022%2C%20more,concentrated%20in%20the%20developing%20world.

**Nikola STANKOVIĆ**

**SAJBER PROSTOR I SUVERENITET U MEĐUNARODNOM JAVNOM PRAVU**

**Apstrakt:** Rad analizira pojavu sajberprostora u kontekstu principa suvereniteta kao fundamentalnog principa međunarodnog javnog prava. Reč je o mladom fenomenu koji se još uvek teško definiše na jasan način u međunarodnoj zajednici. Autor analizira da li se, koji i u kojoj meri formalin izvori međunarodnog javnog prava primenjuju na sajber prostor. Analiza se fokusira na tri centralna izvora međunarodnog javnog prava – međunarodne ugovore, međunarodne običaje i opšta pravna pravila. Sajber prostor se potom analizira iz dva ugla. Prvi, spolji aspekt analize traži odgovor na pitanje da li, pre svega države kao centralni subjekti međunarodnog javnog prava, ali i međunarodna zajednica, i u kojoj meri, imaju suverenitet u sajberprostoru. Drugi, unutrašnji segment analize usmeren je ka utvrđivanju toga da li sajber prostor raspolaže sopstvenim suverenitetom. Rad vrši osvrt i na perspektive vodećih svetskih sila, pre svega Sjedinjenih Američkih Država, Narodne Republike Kine i Ruske Federacije. Autor zaključuje da je neophodno nastaviti sa radom na regulaciji sajber prostora, primarno kroz institucije Ujedinjenih nacija. Jedino regulacija na ovom nivou može obezbediti neophodnu pravnu regulative koja će adekvatno regulisati specifičan prostor kakav predstavlja sajber prostor.

***Ključne reči:*** nadležnost, država, međunarodna zajednica, tehnologija, digitalizacija, vlast.