Advances in Social Science, Education and Humanities Research, volume 498
Proceedings of the XIV European-Asian Law Congress "The Value of Law" (EAC-LAW 2020)

Sovereignty in Cyberspace: A Scholarly and Practical Discussion

Dmitry V. Krasikov[1,2,*], Nadezhda N. Lipkina[1]

[1] *International Law Department, Saratov State Law Academy, 410056 Saratov, Russia*
[2] *Department of law, Institute of Scientific Information for Social Sciences of the Russian Academy of Sciences (INION RAN), 117997 Moscow, Russia*
[*]*Corresponding author. Email: krasikovdv@list.ru*

ABSTRACT
Sovereignty is a central principle of modern international law and is traditionally defined as the supreme power of a state within its territory. While acknowledging the applicability of the principle of sovereignty to the relations between nations in cyberspace, states attach different importance to the concept of sovereignty in the context and characterize it differently. Also, translated into cyber context, the traditional principle of sovereignty has become the subject of debate about its legal nature, about the obligations it engenders, and about its observance. The article reveals the main approaches to scholarly and practical understanding of the principle of sovereignty in the context of cyberspace. The authors refer to the positions of individual states and the opposing opinions of commentators regarding the role of the principle of sovereignty in regulating the behaviour of states related to the use of information and communication technologies and regarding its content. The article also focuses on addressing States' comments on the Initial "Pre-draft" of the report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) that show divergent views on international law applicability in cyberspace. The question of how exactly the principle of sovereignty is applied to cyber relations is highlighted as a key issue in the discussions.
Keywords: *cyberspace, principle of sovereignty, international law, Tallinn Manual 2.0, OEWG*

1. INTRODUCTION

The issues of legal regulation of using information and communication technologies are among the most debatable in modern legal theory. Lately the perspectives of their discussion have changed significantly: the risks that are posed by the new technologies involvement in various social processes have become more clear, a more thorough understanding of the nature of the so-called "cyberspace" and relations in this area has emerged [1], and understanding of utopianism of ideas on exclusive novelty of relationships in cyberspace, on development of an autonomous system of "cyber law" [2] or on the Internet freedom from any governmental interference [3] has crystallized.

On the one hand, many existing legal mechanisms consistently prove their suitability for regulating cyber relations, and on the other hand, the peculiarities of the cyber sphere inevitably raise discussions on adapting the current legal instruments to new reality. International legal norms and institutions are no exception. Their implementation in the field of interstate relations concerning the use of information and communication technologies poses serious issues, and the role of the principle of sovereignty in modern legal architecture of cyberspace lies at the heart of current scholarly and practical discussions.

According to the 2013 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (the GGE), "international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment <…> [and] State sovereignty and the international norms and principles that flow from it apply to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure with their territory". A similar position is set forth in the 2015 Report of the GGE.

As a starting point for assessing the effect of the principle of sovereignty in cyberspace, this position does not raise any doubts. At the same time, as the content of the academic discussion in this area and the relevant practice of various states show, there is no consensus of how this principle is implemented in cyberspace.

The issue is complicated by the uncertainty and inconsistency of approaches to the legal nature of this principle. In particular, questions arise about the existence of an independent value of this principle as a source of obligations of states, about the relationship of this principle with those of the prohibitions on the use of force and of non-interference in the internal affairs of other states, as well as

about assessment of the states' behaviour in cyberspace through the prism of sovereignty.
This article reveals the main approaches to scholarly and practical understanding of the principle of sovereignty in the context of cyberspace.

2. STATES' APPROACHES TO SOVEREIGNTY IN CYBERSPACE: DIVERGENT VIEWS

Sovereignty is a central principle of modern international law and is traditionally defined as the supreme power of a state within its territory. A significant number of institutions and principles of international law directly or indirectly arise from state sovereignty, including the principles of jurisdiction, state immunity, non-interference in the internal affairs of other states, etc.
While acknowledging the applicability of the principle of sovereignty to the relations between nations in cyberspace, states attach different importance to the concept of sovereignty in the context and characterize it differently. The most illustrative example is how the US on one side and Russia and China on the other employ the sovereignty concept in their national and international cyber strategies.
In 2018 National cyber strategy of the United States of America the term "sovereignty" is mentioned only to emphasize that "[the US'] competitors and adversaries <…> hide behind notions of sovereignty while recklessly violating the laws of other states by engaging in pernicious economic espionage and malicious cyber activities, causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world".
The 2011 US International strategy for cyberspace "Prosperity, Security, and Openness in a Networked World" the sovereignty principle was not even mentioned.
In contrast, a significant role to sovereignty is assigned by the 2016 Doctrine on information security of the Russian Federation. Also, in the 2016 Joint statement between the Presidents of the People's Republic of China and the Russian Federation on cooperation in information space development it is emphasized that the parties will "jointly advocate respect to and oppose infringements on every country's sovereignty in information space".
Similarly, China assigns sovereignty an important role in regulating the cooperation of states in cyberspace. Its 2017 International Strategy for Cooperation in Cyberspace advocates the principle of sovereignty as one of the four basic principles of international interaction in cyberspace (along with the principles of peace, shared government and shared benefits).
The document emphasizes the status of the principle of sovereignty as a basic norm in contemporary international relations, and states that "countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies". Noteworthy is the right of states mentioned in this act to "participate in international cyberspace governance on an equal footing" (which may be seen as corresponding to the concept of sovereign equality enshrined in the art. 2(1) of the UN Charter).
The current "asymmetry" between developed and developing countries in the possession of resources and management capabilities in global cyberspace is a matter of concern for Chinese researchers: for example, Yi Shen argues that the way the US ensure its cyber sovereignty amounts to expanding it into Global Cyberspace, while China prefers "to launch the cyber sovereignty defensively" [4].
Despite the fact that the position of states regarding the role of sovereignty in cyberspace and the legal nature of the principle of sovereignty differ, according to experts, national cyber strategies of many states show that "sovereignty is always recognized, and more often than not in a way that indicates it being seen as a rule that can be subject to violations" [5].

3. THE SCHOLARLY DEBATE ON THE LEGAL NATURE OF SOVEREIGNTY

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations [6] (a guide on how existing International Law applies to cyber operations drafted by an international group of experts) (hereafter – Tallinn Manual 2.0.) introduced a rule according to which "A State must not conduct cyber operations that violate the sovereignty of another State." (Rule 4).
Thus, the authors proceed from an understanding of sovereignty as a regulatory norm of international law. The commentary to this rule reflects on two bases for assessing lawfulness of remote cyber operation in the context of sovereignty: "(1) the degree of infringement upon the target State's territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions" [ibid.].
This approach has given rise to a debate regarding legal nature of the sovereignty principle and its application to cyberspace. According to Gary P. Corn and Robert Taylor, while "both custom and treaty, international law establishes clear proscriptions against unlawful uses of force and prohibits certain interventions among states <…> [and] provide a reasonably clear framework for assessing the legality of state activities in cyberspace above these thresholds, including available response options for states", "there is insufficient evidence of either state practice or *opinio juris* to support assertions that the principle of sovereignty operates as an independent rule of customary international law that regulates states' actions in cyberspace" [7].
In the authors' opinion, the law and state practice show that sovereignty presents in itself a principle of international law that establishes the basis for states' interaction but does not have a character of a legally binding rule of international law [ibid.].
At the same time Gary P. Corn and Robert Taylor seem to acknowledge an open character of the principle and its

potential to develop noting that "its consequences are not fully formed in this area" [ibid.].

It is evident that this approach is different from that of the Tallinn Manual 2.0. authors, and the reaction from the leading experts involved in its drafting was not long in coming. Michael N. Schmitt and Liis Vihul came out with arguments that sovereignty is a primary norm of international law and the obligations conferred on states by this norm are independent from those stemming from the rules on prohibition of use of force and on non-interference into domestic affairs [8, 9]. Nevertheless, the authors acknowledge the absence of generally recognized and clear criteria for interpretation of principle of sovereignty in the context of cyber operations [9].

The approach reflected in the Tallinn Manual 2.0. corresponds with general understanding of sovereignty in international law. The two axes along which the analysis was conducted – "the degree of infringement upon the target State's territorial integrity" and "an interference with or usurpation of inherently governmental functions" – are consonant with the provisions of the 1970 Declaration on Principles of International Law Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations which provides for inviolability of territorial integrity and political independence of states.

They are also consistent with the 1975 Conference on Security and Co-operation in Europe Final Act provisions on sovereignty ("The participating States will respect each other's sovereign equality and individuality as well as all the rights inherent in and encompassed by its sovereignty, including in particular the right of every State to juridical equality, to territorial integrity and to freedom and political independence").

However, this does not mean that the Tallinn Manual 2.0. authors have provided a clear picture of how the sovereignty rule is applied in the cyber context. The experts did not find a common position on certain aspects of the application of sovereignty, and these issues remain open within the Tallinn Manual 2.0. framework.

Essentially, the differences in the aforementioned approaches result from differences in the premises from which the authors proceed. At the same time both sides of the debate acknowledge the fact that the principle of sovereignty in its application to interstate relations in cyberspace is at the formation stage and requires further efforts of individual states and of the international community in the development and recognition of relevant practices that can become evidence of due construction of the existing rules or of modification of legal regulation in this area.

Despite the absence of a general consensus among scholars and states regarding individual elements of the content of the principle of sovereignty in cyberspace, recognition of the non-absolute nature of this principle opens up opportunities for dialogue and for searching mutually acceptable solutions.

4. THE WAY FORWARD

4.1. States' comments on the Initial "Pre-draft" of the report of the Open-ended Working Group

The debate on principle of sovereignty is ongoing today, as are the discussions on different issues of application of international law in cyber space.

These discussions are complicated by the fact that, given the differences in the positions of states, as well as the reluctance of some states to express their position on controversial issues [10], even the starting points of the debates have not been definitively determined. Recognition of the applicability of international law to the states' conduct related to using information and communication technologies is often perceived as given, as a kind of presumption.

Nevertheless, the more open the dialogue between states, the easier it is to see that some states oppose even this proposition. States' comments on the Initial "Pre-draft" of the report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (hereafter – OEWG) show divergent views on international law applicability in cyberspace (available at the OEWG portal https://www.un.org/disarmament/open-ended-working-group/).

For example, Venezuela argues that it is necessary to clarify in the report that "International Public Law cannot be directly applicable to cyberspace". Indonesia believes that "automatic" application of existing law without examining the context and unique nature of activities in cyberspace should be avoided. Nicaragua claims about "poor" applicability of existing international law to the field of information and communication technologies.

These and some other states insist on considering new legal instruments addressing cyber issues. According to China, "the view that "existing international law, complemented by the voluntary, non-binding norms that reflect consensus among States, is currently sufficient" is obviously inconsistent with the current situation and existing consensus". The Russia's point of view is that there exists a *de facto* "legal vacuum" in regulating the use of information and communication technologies and that the time is ripe for developing new international legal norms to regulate the states' conduct in cyberspace. Iran, Pakistan, Zimbabwe express basically the same views.

In contrast, most other states argue that the existing international legal framework supplemented by voluntary and non-binding norms of responsible state behaviour in the use of information and communication technologies is sufficient to address all the risks and threats posed by the new technology.

The US characterises the proposals for progressive development of international law in the area as lacking specificity and impractical.

The EU and its Member States note that as for today they "do not see the necessity for the establishment of any structure to develop any new international legal instrument for cyber issues". They express concern "about the risk of entering into a divisive and lengthy process with no substantive and constructive result which risks undermining the ongoing practical efforts to tackle the real, pertinent and pressing problem of increasing cyber incidents, and also risks impacting on work aimed at preventing conflict prevention and promoting stability in cyberspace".

Norway is of the opinion that "while international law has its roots in a time preceding the evolvement of cyberspace, there is nothing new or unique in applying the rules of international law to new areas, following new technological developments. The existing framework of international law must be interpreted in the usual way".

On the one hand, it is obvious that a mere recognition of the applicability of existing international legal instruments to the states' conduct in cyberspace (even if most of the states agree) does not indicate recognition of its sufficiency and effectiveness. No state claims international law to be perfect. On the other, the current challenges posed by technology development require urgent responses and the perspective to start negotiating a new instrument is clearly not among them.

The states' comments on the Initial "Pre-draft" of the OEWG's report also reveal differences in national priorities regarding participation in inter-state dialogue on cyber. The differences in the positions of states regarding human rights and gender issues in the joint work agenda are highly indicative.

4.2. The issue on how international law applies to cyber relations

In these circumstances, in the context of existing differences in the views of states, the main question that forms the main directions of the perspective discussion is the question of how current international law is applied to the behaviour of states in this area. And the matter of more or less established consensus is that the states should answer this question (in its comment on the Initial "Pre-draft" of the OEWG's report China expressed an opposing view: "China is concerned about the proposals to create a "global repository of State practice in the application of international law" and regional exchanges of views and development of common understanding on the application of international law. Our pressing task should be to have in-depth discussions and reach universally-accepted consensus on application of international law, rather than to engage in self-explanations at regional levels or among a small group of countries, expand division and undermine trust).

This question is at the center of efforts to coordinate joint measures aimed at eliminating existing and potential threats in the field of information security within the framework of the United Nations (as acknowledged both by the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security and by the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security), and it has become highly relevant in scholarly discussion.

Commentators argue that the recognition by states of the applicability of existing international law in cyberspace is not a big step forward in itself, the more challenging issue is to understand how the law is applied to specific types of cyber activity, while states rarely express their positions on this subject [11–13].

Indicative in this regard is the position of Harriet Moynihan, an associate fellow in the International Law Programme at Chatham House: "States have agreed that international law, including the principles of sovereignty and non-intervention, does apply to states' activities in cyberspace. But how the law applies is the subject of ongoing debate. Not only is the law in this area unclear; states are also often ambiguous in invoking the law or in how they characterize it" [14]. Thus, the question of how the law is applied is seen as related to the content of the law.

Noting the absence of an agreement on how the law is applied (the law that itself is actually based on agreement or on state practice), Harriet Moynihan calls for a discussion to focus on how the rules applied to practical examples of cyber operations involving states and encourages states to express their views with specific examples. The author believes that "there is likely to be more commonality about specific applications of the law than there is about abstract principles".

On the one hand, the question of how international law is applied to relations in cyberspace is obviously not a question of the methodology of applying law. On the other hand, such a characteristic of applicable international legal instruments as "abstract principles" translates the issue under consideration into a discussion of the legal nature of certain international legal rules, the content of specific norms and principles and their relationship with other international legal rules of conduct.

The behaviour of states in specific circumstances or their abstract expression of relevant positions regarding appropriate conduct and appropriate responses help to understand the content of principles and norms, to interpret them, or they can determine their existence (in the form of customs).

In other words, the discussion on how the rules are applied concerns not only application of law but their legal nature, their content and even their existence. The discussion regarding doubts about the *lex lata/lex ferenda* character of the rules included in the Tallinn Manual on the International Law Applicable to Cyber Operations and the Tallinn Manual 2.0 [10, 15] is an illustration of the complex nature of the issue on how the law applies. It can be noted that one of the US' arguments against taking the proposals for the progressive development of international law (concerning the use of information and communication technologies) seriously by the OEWG is that "without a clear understanding of States' views on how existing international law applies to ICTs, it is premature to suggest

that international law needs to be changed or developed further".

5. CONCLUSION

To date, the theory and practice of international law has developed a more or less stable consensus regarding the applicability of international law to the behaviour of states related to the use of information and communication technologies. Although individual states suggest considering the adoption of new rules of international law that are specifically designed for applying in a cyber context, the main issue of discussion among scholars and states is the question of how existing international law applies in this area.

The discussion on principle of sovereignty is perfectly illustrative of the point. Without denying the applicability of the principle of sovereignty in a cyber context, states assign different meanings to this principle, express divergent positions on its content, and questions remain whether it creates any obligations and what operations may be considered as violating it. These are questions that directly relate to the legal nature and content of this principle, and that have crystallized to date and are waiting for an answer from states.

ACKNOWLEDGMENT

The present paper is a part of the project "Theory-to-practice model of endorsement of territorial sovereignty and delimitation of States' jurisdictions in cyberspace" supported by the Russian Foundation for Basic Research (RFBR Grant No. 20-011-00806).

REFERENCES

[1] J.M. Moringiello, W.L. Reynolds, New territorialism in the not-so-new frontier of cyberspace, Cornell law review 99(6) (2014) 1415–1440.

[2] D.R. Johnson, D. Post, Law and Borders: The Rise of Law in Cyberspace, Stanford Law Review 48(5) (1996) 1367-1402. DOI: https://doi.org/10.2307/1229390

[3] J.P. Barlow, A Declaration of the Independence of Cyberspace, in: P. Ludlow, Crypto Anarchy, Cyberstates, and Pirate Utopias, Cambridge, Mass., MIT Press, 2001, pp. 27–30. DOI: https://doi.org/10.7551/mitpress/2229.003.0006

[4] Y. Shen, Cyber sovereignty and the governance of global cyberspace, Chinese Political Science Review 1 (2016) 81–93. DOI: https://doi.org/10.1007/s41111-016-0002-6

[5] A. Väljataga, Tracing opinio juris in National Cyber Security Strategy Documents, NATO CCD COE, 2018.

[6] M.N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

[7] G.P. Corn, R. Taylor, Sovereignty in the age of cyber, American Journal of International Law Unbound 111 (2017) 207–212. DOI: https://doi.org/10.1017/aju.2017.57

[8] M.N. Schmitt, L. Vihul, Sovereignty in cyberspace: lex lata vel non? American Journal of International Law Unbound 111 (2017) 213–218. DOI: https://doi.org/10.1017/aju.2017.55

[9] M.N. Schmitt, L. Vihul, Respect for sovereignty in cyberspace, Texas Law Review 95(7) (2017) 1639–1670.

[10] D. Efrony, Y. Shany, A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice, American Journal of International Law 112(4) (2018) 583–657. DOI: https://doi.org/10.1017/ajil.2018.86

[11] B.J. Egan, International Law and Stability in Cyberspace, Berkeley Journal of International Law 35(1) (2017) 169–180.

[12] H.H. Koh, International Law in Cyberspace. Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012, Harvard International Law Journal Online 54 (2012) 1–12.

[13] F. Delerue, Cyber Operations and International Law, Cambridge University Press, 2020.

[14] H. Moynihan, The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention, The Royal Institute of International Affairs Chatham House, 2019.

[15] L.J.M. Boer, Lex Lata comes with a Date; or, What Follows from Referring to the "Tallinn Rules", American Journal of International Law Unbound 113 (2019) 76–80. DOI: https://doi.org/10.1017/aju.2019.11