ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVI/SUPLIMENT, ŞTIINŢE JURIDICE, 2020

Limits of International Law in a limitless Cyberspace. Challenges and uncertainties

Limite ale dreptului internaţional în spaţiul cibernetic fără limite. Provocări şi incertitudini

Carmen Moldovan[1]

Rezumat: Scopul prezeneti lucrări este de a evidenţia asimetria dintre dinamica permanentă a stapţiului virtual (lnd în considerare trăsărutile sale particulare şi posibile definiţii) şi procesul lent de dezvoltare şi cristalizare a unor reguli speciale ale dreptului international în acest domeniu. Cu toate acestea, lucrarea susţine că nu există un decalaj normativ real şi va explora rezultatele activităţii de cercetare a diferitelor organisme şi grupuri de experţi în acest sens, în special a grupurilor de lucru speciale create în cadrul Naţiunilor Unite şi NATO. Ca urmare a evoluţiilor legale recente referitoare la spaţiul virtual, este general acceptat faptul că dreptul internaţional este aplicabil operaţiunilor cibernetice, însă nu există deocamdată indicii cu privire la modul în care aceastea se aplică în mod concret. Aceasta este una dintre cele mai mari provocări ale dreptului internaţional în acest moment. Tehnologia şi spaţiul virtual sunt, în fapt, supuse unor reglementări limitate ale statelor datorită dezvoltării lor constante şi extrem de dinamice. Ciberspaţiul este un mediu extrem de explorat şi utilizat; iar nevoia normativă a statelor este justificată. Cu toate acestea, nu se poate contesta faptul că regulile apar *post factum* şi, deşi pare dificil să se adapteze la situaţii noi şi existente, procesul acesta de adaptare în legătură cu spaţiul virtual prezintă un grad mai ridicat de dificultate având în vedere că normele ar trebui să se aplice pentru viitor şi, în acest sens, singura certitudine este evoluţia continuă a spaţiului cibernetic.

Cuvinte-cheie: sursele dreptului internaţional; trăsăturile spaţiului virtual; jurisdicţie; responsabilitate.

Abstract: The aim of this paper is to address the asymmetry between the constant dynamic of Cyberspace (taking into consideration its special features and possible definitions) and the slow development of special International Law rules in this regard. However, the paper submits that there is not a normative gap and will explore the results of the research work of different bodies and expert groups in this regard especially the special working groups created within the United Nations and NATO. As a result of recent legal developments concerning Cyberspace, it is generally accepted that International Law is applicable to cyber operations, yet there are no indications on

[1] Lector univ. dr., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza”, Iaşi, e-mail: carmen.moldovan@uaic.ro.

how this process is happening. And this is one of the greatest challenges of International Law at the moment.

Technology and Cyberspace are in fact subject of limited State regulations due also to their constant and highly dynamic development. Cyberspace is a highly explored and used environment; and the normative need is justified. However, one cannot dispute that the law is always post factum and although it appears difficult to adapt to new and existing situations, the process is more difficult taking into consideration that the rules should apply for the future and in this regard, the only certainty is the continuous evolution of Cyberspace.

Keywords: sources of International Law; Cyberspace features; jurisdiction; responsibility.

Introduction

Cyberspace is one of the most remarkable creations of mankind, and its continuous development and evolution have contributed to serious changes in all areas of social interaction, allowing the transmission of data and information quickly, without any physical borders. The special dynamics have determined a continuous expansion of this environment with respect to which several terms as *cyber space, digital space*, *virtual space* used as equivalents, without being comprehensively defined. It should be noted that this environment is the result of the creativity of private, non-state entities, states being relatively recently interested in identifying the rules applicable here. This concern coincides with the use of the Internet and digital space to commit attacks on States or private companies or to undertake activities that either influenced the electoral process or aimed at misinformation or the dissemination of fake news.

Recent works adopted within the United Nations and NATO[2] in particular, stating the applicability of International Law in this environment put an end to the debates about the free and unregulated nature of the Internet and consequently of the virtual space at the international level or through the actions of States. Until their adoption, Cyberspace was considered to be a grey area or outside the rules of International Law, unregulated and uncharted, or even an anarchic and disorganized environment[3]. At date, this assertion is no longer founded, due to the recognition, at universal as well at regional level, of the application of rules and principles of International Law.

[2] M. Tolppa, O*verview of the UN OEWG developments: continuation of discussions on how International Law applies in cyberspace,* 2020, https://ccdcoe.org/library/publications/overview-of-un-oewg-developments-continuation-of-discussions-on-how-international-law-applies-in-cyberspace/ accessed 10 November 2020.

[3] S. Arsène, *Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order?* in China Perspectives 2016/2 | 2016 What Kind of International Order Does China Want, 2017, p. 28.

All recent reports agree on the applicability of principles of International Law to State behaviour in Cyberspace (especially sovereignty, non-intervention and cooperation). However, no matter how elaborate and complex some of these reports are, there is no indication on how these well-established and traditional principles of International Law should actually apply. An international treaty on Cyberspace is unlikely in the foreseeable future, therefore existing rules, *soft law* and International Customary Law may give answers to sensitive issues on which States are silent or ambiguous. At the same time, States should consider the acts and rules of non-state entities and private actors and establish a balance between the existing norms and the future implications of cyber development.

From the technical perspective, hardware and software, there are no limits in the expansion of Cyberspace, it will evolve according to the progress of communication technologies and at this moment it is very difficult to anticipate what the future evolution of Cyberspace will be and the extent of cyber activities of States.

From the legal perspective, there are no impediments to its continuous development, therefore Cyberspace may be considered limitless.

1. Is Cyberspace *res communis omnium*?

The fact that the Cyberspace and the Internet are for the most part privately owned poses the risk for the existing International Law rules and their safeguards for private individuals not to be applied, as rules of Public International Law regulate firstly the behaviour of States and in some areas such as the Human Rights Law, they contain special safeguards for individuals.

However, we should take into consideration another possibility: the change of paradigm by accepting the idea that Cyberspace is regulated by multi stakeholders and that normative competence is not just the prerogative of the States[4]. It is however very unlikely that States will accept such a possibility as it would mean the loss of their exclusive capacity to regulate and define International Law (to act as a legislator) – which involves the adoption of rules in those areas desired by States, depending on the interests they may have or pursue at a certain time.

It must be emphasised that the reports of the UN special working groups do not codify norms of international law, a possibility recognized for the International Law Commission and for the States and regulating Cyberspace appears to be in its beginning phase.

Development of communication and information technology presents great advantages for humanity and all types of relationships yet at the same

[4] A. van der Spuy, *What if we all governed the Internet?Advancing multistakeholder participation in Internet governance*, UNESCO Series on Internet Freedom, 2017, p. 26.

time it may be used with the objective of causing harm or be detrimental to the normal exercise of human rights. The disclosure made by Edward Snowden in 2013 about the internet mass surveillance program of the US National Security Agency (NSA) revealed that technologies may be used in breach of the rights of private persons and that they may be vulnerable to other States' dominance in the field of information and communication technologies.[5] The disadvantages of Cyberspace and its free character does not encompass only technical vulnerabilities but is may extend to data on classified information of the State affecting its national security or it may concern data on the population or even be used as a means of misinformation or disinformation. Such situations completely justify the interest of the State in protecting its ICT infrastructure and data integrity. Related on this issue is the concept of cyber sovereignty promoted especially by China and Russian Federation. The purpose of this paper is not to analyse this concept.

2. Features and possible definitions of Cyberspace

The origins of the term Cyberspace and the best description of this environment are found in the 1984 book *Neuromancer* of William Gibson which is focusing on complex flux of information and data[6]. The difference between it and the actual status of Cyberspace is a qualitative one, as it is a type of interaction of humans and technology which lacks the connection between the human conscience and computers.

The virtual space is used for civil and for military purposes at the same time and it grants a high degree of anonymity. It is a logical space which is actually difficult to be accurately perceived and managed, unable to exist without support from the physical world, meaning the physical infrastructure[7]. Yet there is no consensus on what this environment is and users may be looking at it and understanding its functions and implications differently[8].

The ordinary sense of Cyberspace may be one or more of the following:

[5] M. Baezner, P. Robin, *Trend Analysis: Cyber Sovereignty*, Risk and Resilience Team Center for Security Studies (CSS) ETH Zürich, 2018, p. 6.

[6] "*Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding" - Neuromancer* (first published 1984 Ace Books).

[7] Y. Shen, *Cyber Sovereignty and the Governance of Global Cyberspace*, Chin. Polit. Sci. Rev., 2016, 1:81–93, p. 84

[8] Eds. D. Broeders, B. van den Berg, *Governing Cyberspace: Behavior, Power, and Diplomacy*, Rowman & Littlefield, 2020, p. 2

"the internet considered as an imaginary area without limits where you can meet people and discover information about any subject; an electronic system that allows computer users around the world to communicate with each other or to access information for any purpose; the internet considered as an imaginary area where emails, websites, etc. exist, especially when information is passing between one computer and another"[9] or the online world of computer networks and especially the Internet[10] or to describe the virtual world of computers[11]; "Cyber-space is nothing more than a symbolic and figurative space that exists within the scope of the Internet."[12]; "Cyber-space is nothing more than a symbolic and figurative space that exists within the scope of the Internet."[13].

According to one proposed definition "cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems."[14] This feature is highly relevant as it stresses the dynamic of cyberspace and its constant possible changing.

Another essential feature of Cyberspace is its "border lessness" that is not is not just geographic but also limits between issues that should be regulated by a formal system of States[15] and those that fit better for self-regulation or international cooperation are challenged by the physical nature of the spaces.

A definition that captures all these essential features of Cyberspaces is given by the 2020 *DOD Dictionary of Military and Associated Terms (DOD Dictionary)*[16] which establishes standards for the US military as

A global domain within the information environment consisting of the 'interdependent networks of information technology infrastructures and resident

[9] https://dictionary.cambridge.org/dictionary/english/cyberspace accessed 10 November 2020.

[10] https://www.merriam-webster.com/dictionary/cyberspace accessed 10 November 2020.

[11] https://techterms.com/definition/cyberspace accessed 10 November 2020.

[12] https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html accessed 10 November 2020.

[13] https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html accessed 10 November 2020.

[14] R. Ottis, P. Lorents, *Cyberspace: Definition and Implications, i*n Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited,2010, pp. 267-270.

[15] K.N. Metcalf, *Legal View on Outer Space and Cyberspace: Similarities and Differences*, Tallinn Paper No. 10, 2018, p. 2, https://ccdcoe.org/uploads/2018/10/Tallinn-Paper_10_2018.pdf accessed 10 November 2020

[16] *DOD Dictionary of Military and Associated Terms* as of June 2020, p. 54 https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf accessed 10 November 2020.

data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12).

It also defines terms such as *cyberspace attack*, *cyberspace capability, cyberspace defense, cyberspace exploitation, cyberspace operations, cyberspace security, cyberspace superiority*[17].

The US military definition of Cyberspace is consistent with the idea of an open and global environment that could be qualified as *res communis omnium.* However, it must be noticed that the scope of all these definitions is limited to the military dimension of Cyberspace.

3. What are the rules of International Law applicable in Cyberspace?

Through the lenses of International Law, Cyberspace may appear as unregulated and uncharted as there lacks binding legal instruments. Consequently, one could argue that it is an anarchic and disorganized environment. In order to be able to qualify a State conduct as legal or not, first it is necessary to identify the meaning, the scope and the potential limits of a specific rule setting a certain conduct for States.

As an exception, the *Budapest Cybercrime Convention*[18] adopted is the only biding legal instrument, yet its scope is limited to acts committed by individuals, provides a framework for State cooperation in the field of computer and Internet related crimes, child pornography and violation of security network; it is a regional legal instrument adopted within the Council of Europe and it does not regulate issues concerning the responsible conduct of States in Cyberspace. Its additional Protocol concerns criminalisation acts of a racist and xenophobic nature committed through computer systems[19].

The process of identifying cyber norms began after 1998, when the Russian Federation submitted to the General Assembly a resolution on "Developments on the Field of Information and Telecommunication" to the UN`s First Committee[20], calling for dialogue between States[21].

[17] *DOD Dictionary of Military and Associated Terms* as of June 2020, pp. 55-56.

[18] *Convention on Cybercrime*, Budapest, 23 November 2001, ETS No.185.

[19] *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems,* Strasbourg, 28 January 2003, ETS No.189.

[20] UN General Assembly, *Developments in the field of information and telecommunications in the context of international security: revised draft resolution / Russian Federation*, A/RES/53/70, 2 November 1998, https://digitallibrary.un.org/record/263069?ln=en#record-files-collapse-header accessed 10 November 2020.

All forms of rules proposed on cybers activities of States – reports, statements of best practices, codes of conduct, scholarly works are not legally binding and in a generic manner, all could be included in the category of *soft law.* The effort of codifying rules is highly difficult due to the complex nature of cyberspace, and it must be appreciated.

The main legal consequence of this situation is the fact that their violation does not determine the international responsibility of States (in the sense of the *Draft Articles on State Responsibility for International Wrongful Acts*[22]) and does not involve the same legal remedies. For example, as a general rule, a breach of an international obligation gives rise to reparations. Applying this principle to cyberoperations, if a State`s cyber activity violates another`s State sovereignty, the victim State has the right to reparations and the right to countermeasures. Not least, if the breach may be considered that it trespasses the threshold of an armed attack, it may justify the exercise of legitimate self-defence in the sense of Article 51 of the UN Charter[23]. Responsibility remains an open subject taking into consideration the difficulties in establishing the imputability of the illegal conduct.

The most appreciated results in identifying Cyber Norms belong to group of experts or working groups established either by NATO (Cooperative Cyber Defence Centre of Excellence -CCDCOE), General Assembly (Group of

[21] L. Adamson, *International Law and International Cyber Norms. A continuum?*, in *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by D. Broeders and B. van den Berg, Rowman & Littlefield, 2020, p. 19.

[22] International Law Commission, *Draft Articles on State Responsibility for International Wrongful Acts,* 2001 https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf, accessed 10 November 2020

[23] Article 51 of the UN Charter reads as follows: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security." Charter of the United Nations, 24 October 1945, 1 UNTS XVI. The Charter was signed at San Francisco on 26 June 1945. The amendments included here are: Amendments to Articles 23, 27 and 61, 557 UNTS 143, adopted by the General Assembly Resolutions 1991A and B (XVIII) of 17 December 1963, entered into force on 31August 1965 for all Members; - Amendment to Article 109, 638 UNTS 308, adopted by the General Assembly Resolution 2101 (XX) of 20 December 1965, entered into force on 12 June 1968 for all Members; Amendment to Article 61, 892 UNTS 119, adopted by the General Assembly Resolution 2847 (XXVI) of 20 December 1971, entered into force on 24 September 1973 for all Members.

Governmental Experts, Open-ended Working Group) or proposed by the private sector like Microsoft (who developed the Digital Geneva Convention).

Within the United Nations[24], the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) was created in 2004 having at the beginning 10 member States. Currently, it has 25 members. The GGE reports to the General Assembly of the UN. Several sessions were held and the most important are those from 2013 and 2015 when it stated that the principles of the UN Charter apply to states' conduct and operations in cyberspace. These findings are especially relevant because they put an end to the controversy if International Law is applicable or not to cyber operations and activities.

The Open-ended Working Group[25] was created due to the deadlock of the UNGGE in 2017, when it was not able to find consensus on how International Law applies to cyber operations.

One of the most relevant conclusions of the 2013 Report of the UN GGE are

> "*that 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…*"

> "*that 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*"

and

> "*State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.*"[26]

The report directly relates sovereignty and international norms to ICT related activities and jurisdiction of states over ICT infrastructure

[24] *Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,* https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf, accessed 10 November 2020.

[25] UN General Assembly (2018), *"Resolution adopted by by the General Assembly on 22 December 2018 on "Advancing responsible State behaviour in cyberspace in the context of international security"*, UN Doc A/RES/73/266, https://undocs.org/en/A/RES/73/266 accessed 10 November 2020.

[26] UN General Assembly General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013.

The 2015 UN GGE Report confirms the rules and principles found applicable by the previous report:

> "*24. The 2013 report stated that international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. Pursuant to its mandate, the present Group considered how international law applies to the use of ICTs by States.*
>
> *25. The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment. These obligations are central to the examination of the application of international law to the use of ICTs by States.*"[27]

The findings of these reports are important for the activity of the UN and for ending the debate on the totally free and unregulated Cyberspace. Yet, a more thorough look into this works reveal that its effects are actually limited; they enunciate the basic principles of International Law without providing any detail of their content and sense. From the lenses of legal consequences, the findings of the UN GGE have the meaning of recommendations.

For the process of identifying rules of International Law applicable in Cyberspace *Tallinn Manual* 2.0[28] has an important contribution and is considered the most comprehensive guide on the applicability of International Law to cyber operations.[29] The previous version of the Tallinn Manual focused on issues related to cyber warfare[30], therefore, an evolution must be acknowledged regarding the extent to which International Law applies.

One should note that there are quantitative and qualitative differences between all research results meaning that the conclusions concern special legal concepts and applicability in regard to certain topics. Tallinn Manual is very relevant in assessing how legitimate self-defence could apply in cyberspace, and in setting criteria of qualifying a cyber-attack as an armed attack. The UNGGE stressed the applicability of principles, norms and rules of International Law in ambiguous terms.

---

[27] UN General Assembly A/70/174, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2015, paras 24, 25.

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

[29] E.T. Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, Georgetown Journal of International Law, Volume 48, 2017, pp. 735-778.

[30] Ed. M.N. Schmitt, *Tallinn Manual on the on the International Law Applicable to Cyber Warfare,* Cambridge University Press, 2013.

On the other hand, the private actors were more active and more courageous in regulating different aspects of users conduct in the digital space. *Digital Geneva Convention*[31] proposed by Microsoft in 2017 is an example of private actors' implications in the attempt[32] to regulate different dimensions of State operations. The Digital Geneva Convention tackles issues concerning a humanitarian approach of cyberspace in reaching cyber stability, yet the relevance of international humanitarian rules and their connection to usual actions in cyberspace is not apparent or obvious as not all international humanitarian rules may be applicable – protection of war prisoners, how it is possible to identify the victims, to discriminate between civilians' targets and military targets.

4. Solutions for filling in the normative gaps

In addressing the issue of sources of cyber norms, the provisions of Article 38 of the Statute of the International Court of Justice[33] are the legal framework for discussions and debates.

Concerning the norms on States cyber activities and the lack of an international treaty, the notion of customary international law was addressed. However, the fact that the UNGGE is currently experiencing deadlock and the lack of a uniform approach from States cannot lead to the conclusion that there

[31] B. Smith, *The need for a digital Geneva Convention*, 17 February 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv, accessed 10 November 2020.

[32] J. Guay, L. Rudnick, *What the Digital Geneva Convention means for the future of humanitarian*, The Policy LabJune 25, 2017, actionhttps://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/, accessed 10 November 2020.

[33] Statute of the International Court of Justice forms an integral part of the Charter of the United Nations, https://legal.un.org/avl/pdf/ha/sicj/icj_statute_e.pdf accessed 10 November 2020.

Article 38 reads as follows:

"1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:

a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;

b) international custom, as evidence of a general practice accepted as law;

c) the general principles of law recognized by civilized nations;

d) subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

2. This provision shall not prejudice the power of the Court to decide a case *ex aequo et bono*, if the parties agree thereto."

is *opinio juris* among Member States. In this regard, the interpretation given by the International Court of Justice in the *Case concerning military and paramilitary activities in and against Nicaragua* is still highly relevant. The Court stated that

> "*In considering the instances of the conduct... the Court has to emphasize that, as was observed in the Noth Sea Continental Shelf cases, for a new customary rule to be formed, not only must the acts concerned 'amount to a settled practice', but they must be accompanied by the opinio juris sive necessitatis. Either the States taking such action or other States in a position to react to it, must have behaved so that their conduct is évidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it. The need for such a belief, i.e., the existence of a subjective element, is implicit in the very notion of the opinio juris sive necessitatis*".[34]

Taking into consideration the apparent normative gaps, general principles of International Law and general principles of law in the sense of Article 38 para 1 d) of the Statute of International Court of Justice may be very useful in solving disputes generated by cyber activities. The applicability of general principles of International Law may not actually be contested even though the Internet and Cyberspace are not created or owned exclusively by States. At this point, there is a significant number of results of working groups or group experts that analysed different legal concepts and their implications over cyber activities. This means that States and non-state actors show concern in regulating this environment in order to ensure the stability and responsible behaviour therein. The common feature of all these works and reports is the applicability of rules and principles of International Law in Cyberspace and to actions conducted by different actors. However, no matter how elaborate and complex some of these reports are, there is no indication on how these well-established rules should actually apply.

Moreover, in solving the gaps regarding the applicability of rules and principles of International Law in Cyberspace and for the conduct of States, an evolutive method of interpretation may be used. In this regard, the provisions of Article 31 (3) b of the 1969 Vienna Convention on the Law of Treaties[35]

[34]ICJ, *Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America*), Merits, Judgment of June 1986, para 207, https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf, accessed 10 November 2020

[35] *Vienna Convention on the Law of Treaties,* concluded at Vienna on 23 May 1969, UNTC No. 18232. Article 31 (3) b reads as follows: "3. There shall be taken into account, together with the context:(b) any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation;(...)".

states may prove relevant in establishing the significance of future State practice.

Final remarks

The main purpose of this paper was to demonstrate that regarding regulation of Cyberspace by International Law, States, non-State entities and private actors are acting on equal positions in the process of clarifying the norms applicable, their content and establishing a balance between the existing norms and the future implications of cyber development. At this point, it appears that Cyberspace may not be subject to full State control or State appropriation and therefore, the competences of States as primary actors in International Law are in fact limited in this environment by the rights of other stakeholders. Issues such as State jurisdiction, responsibility (including establishing the imputability of the illegal conduct) and sovereignty in Cyberspace are very sensitive and ambiguous. Future State practice and diplomatic discussions will play an important role in clarifying the meaning of the rules and principles of International Law applicable to States conduct in Cyberspace. In this special and constantly expanding environment States, non-state entities and private actors are acting on equal positions in the process of clarifying the norms applicable, their content and establishing a balance between the existing norms and the future implications of cyber development. At this point, it appears that cyberspace may not be subject to full State control or State appropriation as the notion of State jurisdiction in this matter is a very sensitive one and unregulated. Therefore, States should establish the limits of the "traditional" principles of International Law in Cyberspace and accept the change of the normative paradigm in regulating Cyberspace.