On the normative equivalence paradigm in cyberspace

Carmen Moldovan[1*]

[1]Faculty of Law, Alexandru Ioan Cuza University of Iași, Romania

Abstract. Constant evolution of communication technology and expansion of Cyberspace has had a pervasive effect on all areas of human life, activities and interactions, that law unsuccessfully tried to regulate. Cyberspace was for a long period of time considered uncharted territory, an unlimited and open space outside the control of States and the limits on the admissible or accepted conduct of states and other stakeholders were blurred. In this context, the most important challenge and pressing need is to identify normative guidelines applicable in this environment considering its specific features (being unlimited, world-wide availability, anonymity). The aim of the paper is to challenge the elements of the so-called normative equivalence that was developed by several international bodies first in relation with human rights safeguards and extended as generally applicable with some special approaches at the level of the European Union (protection of personal data, strategy on cybersecurity) which will not be addressed.

1 Special architecture of Cyberspace

There is no terminological consistency to designate Cyberspace and terms like *cyberspace*, *digital space*, *cyber space* or even *digital ecosystem* [1], are used as interchangeable. Cyberspace is not defined by International Law or used as such, instead the terms "Information and Communication Technology" (ICT) are used and favoured by the United Nations in different reports and documents. The term Cyberspace in the sense used now has its origins in the 1984 book *Neuromancer* by William Gibson, who described it as follows:

'*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*' [2].

Previously, it was used by the Danish artist Susanne Using in the late 1960s when she and the architect Carsten Hoff constituted *Atelier Cyberspace*, which had nothing to do with the current sense given to this term (it represented a series of installations and images entitled "sensory spaces" that were based on the principle of open systems adaptable to various influences, such as human movement and the behaviour of new materials) [3].

* Corresponding author: carmen.moldovan@uaic.ro

Unlike the state territory which has a material and physical dimension, Cyberspace is entirely human made [4] and constitutes a complex global network, a logical space, unlimited, imperceptible, non-materialized, time-dependent [5] and constantly changing, who cannot exist without the physical support of infrastructure [6], an interconnected information system created by non-state actors, with no borders [7], parallel to the physical territory.

All these features make it a *sui generis* phenomenon [8], that it is probably one of the greatest creations of humanity. At the same time, we should highlight that Cyberspace is not only civil and commercial space, it is also a military space being used for military purposes and activities.

In order to justify regulation of Cyberspace, it was characterised as chaotic, anarchic [9] and asymmetric in relation to resources and capabilities in cyberspace [6] that protect the interests of States in relation to other States, affirming this principle does not resolve all the subsequent issues: state responsibility, consequences on the interests and rights of private persons and non-state actors. The complexity of the environment itself, the diversity of its users (States, non-state actors, private companies, private persons) actually determined multiple layers and different types of relationships between its users, depending on their quality and of the nature of the acts. Hence, the environment can be divided technically and legally in several parts: public networks accessible to everyone and not restricted by internal borders, with free access; territorial networks such as military intranets or government networks with limited access; exclusive networks - for e-government services, business, finance - the access is limited to authorised persons [10].

Due to the lack of a standard or objective definition of Cyberspace, it is generally used regarding any aspects of using computer and internet networks [5] and the term "cyber" has been used to describe almost anything that has to do with networks and computers, especially in the security field. Etymological, the term Cyberspace comes from 'cybernetics', which in turn is derived from the Ancient Greek 'kybernētēs', which means 'steersman, governor, pilot, or rudder'. Norbert Wiener defined the term 'cybernetics 'in the title of his book as "Cybernetics: Or, the Control and Communication in the animal and the machine". The idea that humans can interfere with machines and that the resulting system can provide an alternative environment for interaction provides a foundation for the concept of Cyberspace [5].

Legally defining Cyberspace may be impossible due to its dynamic nature and the unpredictability of its future evolution. However, the environment cannot be considered as unregulated or uncharted, rather a regulated as a multistakeholders model [11].

2 Attempts to define and regulate Cyberspace

States did not succeed in the task of completely regulate Cyberspace and to clarify the norms and obligations incumbent to them and to other stakeholders in this environment. There are very few treaties or regional legally binding instruments governing issues of Cyberspace: Convention on Cybercrime [12], its Additional Protocol [13], Shanghai Cooperation Organisation's International Information Security Agreement [14], the International Telecommunication Union Constitution and Convention [15] and International Telecommunication Regulations [16].

All these instruments are limited in scope and terms and do not contain a definition of Cyberspace or of the meaning of state responsible behaviour in this environment. Budapest Convention on Cybercrime has a limited scope to criminal behaviour of persons through informatic systems and does not clarify the jurisdiction issues. The Shanghai Organization (led by Russia and China) [17] defines cyberwarfare but does not tackle other elements of state behaviour or applicable rules of International Law [18].

It also proposed, in 2015, the International Code for Information [19] with very little effect and reaction from other States. From the perspective of the terms used, the International Code for Information security is interesting, yet it has only a declarative purpose. At least partially and formally, the purpose of this code of conduct is similar to the recommendations established within UN, as it *"is to identify the rights and responsibilities of States in the information space, promote constructive and responsible behaviour on their part and enhance their cooperation in addressing common threats and challenges in the information space, in order to establish an information environment that is peaceful, secure, open and founded on cooperation, and to ensure that the use of information and communications technologies and information and communications networks facilitates the comprehensive economic and social development and well-being of peoples, and does not run counter to the objective of ensuring international peace and security.*" [20]

It refers to the Charter of the United Nations and especially to the principles of sovereignty, territorial integrity and political independence [21]. Overall, it refers to all the rules of International Law that may be related to the cyber activity of States. As opposed to other instruments, this Code uses and focuses on information society, not on cybersecurity [22].

A relevant example of a regional effort in identifying rules applicable to cyber operations is the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (The Tallinn Manual 2.0) [23] considered to be the most comprehensive academic publication on the subject of cyber activities [24]. It contains useful findings concerning the principles of sovereignty and non-intervention in Cyberspace yet, it does not provide an answer to all questions and focuses on issues related to use of force in peacetime, preventive self-defence, cyber-attacks and evaluating imminence of cyber-attacks. As estimated, the Tallinn Manual proved highly influential in matters concerning the activity of States in Cyberspace [25].

There are also several private initiatives on rules applicable in Cyberspace. The *Paris Call for Trust and Security in Cyberspace* [26] was launched in 2018 as a multistakeholder initiative and formulated nine principles - principle number 9 refers to International norms - promotes the widespread acceptance and implementation of international norms of responsible behaviour as well as confidence-building measures in Cyberspace. A *Digital Geneva Convention* proposed by Microsoft in 2017 underlines the importance of international humanitarian law in cyberspace, without giving details on how this is applicable and to what extent and it is at the same time appreciated [27] and criticised [28].

3 Consensus that International Law applies in Cyberspace

As a result of the works of different bodies within the United Nations on norms applicable in Cyberspace, it is generally accepted that International Law is applicable to cyber operations [29, 30] and this consensus puts an end to the controversy in this regard, and to the idea that States should not be involved in regulating this environment and affect the free internet. One legal consequence of this finding is that States should comply with the correlative rights and obligations in their activities therein [31].

The conclusions found in recent *soft law* acts by the United Nations through different working groups [32] refer to voluntarily non-binding norms, rules and principles of responsible state behaviour in cyberspace, that International Law rules apply in cyberspace, the need to implement confidence-building measures to build trust between States, and to increase global capacity when it comes to ensuring cyber security [29]. These reports are considered to be one of the first United Nations initiatives in this regard [33].

The common feature of all legal instruments related to state activity in Cyberspace is that they all recognize that the existing International Law actually provides the framework for

regulating the conduct of States in cyberspace [34]. However, neither of them provides any indication on exactly how this conclusion may be transferred into practice and it cannot be considered as elements of international custom. State practice continues to be ambiguous or silent, although States enjoy the prerogative of engaging themselves in formally adopting rules of conduct applicable in Cyberspace [24].

4 Overview of the relevant conclusions of the UN GGE

Within the United Nations, the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter UN GGE) was created in 2004 [35] as an exclusive body [24] having at the beginning 15 member States: Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, Russia, South Africa, South Korea, United Kingdom, United States of America [36]. Further, a number of 25 States were members of the UN GGE [37]. The GGE reports to the General Assembly of the United Nations. Several sessions were held and the most important ones are those from 2013 [38] and 2015 when it was stated that the principles of the United Nations Charter apply to States' conduct and operations in Cyberspace [41]. Although a small group, its work is generally considered as the first step in identifying cyber norms and addressing the question of responsible behaviour of States in Cyberspace [39].

One of the most relevant conclusions of the 2013 Report of the UNGGE [40] is

"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".

All in all, the report contains recommendations and uses as interchangeable the notions of principle, norms and rules [39]. Despite and beyond this vagueness, the report directly and repeatedly associates state sovereignty and international norms to ICT related activities and jurisdiction of States over ICT infrastructure within their territory. It mentions that it

''offers the following non-exhaustive views on how International Law applies to the use of ICTs by States: (b) In their use of ICTs, States must observe, among other principles of international law, S*tate sovereignty, sovereign equality (....)"*and comply with their international obligations, which corresponds to general rules of international law. [41]

The 2015 UN GGE Report confirms the rules and principles of International Law found applicable by the previous report in similar terms. Moreover, it asserts that it considered how International Law applies to the use of ICTs by States [42] but a thorough lecture and analysis does not reveal clearer issues than the previous ones. The 2015 Report also contains a series of recommendations [43], as voluntary norms, rules and principles for the States' behaviour in Cyberspace. That was the maximum result of the UN GGE because in 2017 it ended in a deadlock as it was not able to adopt a consensus report [44]. The points of divergent views for States were particularly on the right to self-defence and the applicability of international humanitarian law to cyber conflicts. [45]

5 The deadlock of the UN GGE and the creation of the OEWG

From a critical point of view, the findings of these reports are actually limited as they hold the application of International Law rules and enunciate fundamental principles and the need for cooperation between States and other stakeholders in Cyberspace but they emphasize the lack of consensus on how they apply [46], which is the most important issue to be addressed. Moreover, the findings of the UN GGE have at most the meaning of recommendations or *soft law* as a legal nature and the fact that the Group is currently experiencing deadlock cannot lead to the conclusion that there is *opinio juris* among States. As a consequence, the UN

created in 2018 an *Open-ended Working Group* (OEWG) [47] with similar prerogatives. In 2018 also, the UN General Assembly established a new GGE to work on these issues starting from 2019. [48]. In contrast with the UN GGE, the OEWG is inclusive [29], as it is open to all interested United Nations member States, thus creating the possibility for a larger number of States to participate in and express their opinion. Hence it is a more open and accessible framework for discussion.

The objective expressed in resolution A/RES/73/266 *"was to provide all Member States the opportunity to engage in interactive discussions and share their views on issues under the GEE's mandate."* [48].

The first Substantive meeting took place in December 2019 and it found „*broad agreement … that the cumulative outcomes of the previous GGE reports should serve as a basis for discussions in both the GGE and the OEWG*" and established that *„the new GGE should focus on moving beyond what was already agreed in 2015*" and that the 2015 recommendations should be respected [49].

The fact that the UN GGE failed to give clear guidance on how the principles of International Law apply in Cyberspace was considered whether a "blessing in disguise or a major setback" [45]. Yet, this situation does not automatically determine the unregulated character of Cyberspace. All these actions reflect a genuine concern and interest from States and United Nations, yet it is rather unlikely that the future work of international bodies within the United Nations or other international organizations will be clearer on issues connected to cyber sovereignty.

The existence of two working groups having similar mandates may prove inefficient and highly politically influenced. Instead of obtaining transparency and predictability, the position of States could continue to remain ambiguous. The failure in reaching consensus on how International Law applies is determined by the political nature [44] of these special working groups. However, it must be stressed that the role of the reports of the GGE and OEWG is not a normative one because they may not adopt cyber norms [44], a term subject to criticism and considered inappropriate [50].

6 Legal uncertainty on the extent to which rules of International Law is applicable in Cyberspace

The norms regarding State responsible behaviour in Cyberspace, identified by the works of the two working groups are generally considered norms voluntarily accepted by States [42]. This assertion is partially inadequate and presents the great disadvantage of their non-binding force; therefore, they are not part of the *hard law* and no international obligations may derive from them. Such an assertion is highly relevant as an example, from the perspective of applying the sovereignty principle in Cyberspace, for establishing jurisdiction and other legal consequences. Therefore, these conclusions lead to legal uncertainty.

However, works of the OEWG highlight the essential role of the 2015 Report of the UN GGE, the need for the implementation of the voluntary norms identified in order to ensure the public core of the internet, all through a human rights approach [51]. Furthermore, on 30th October 2020, the document *The future of discussions on ICTs and Cyberspace at the UN* [52] of the OEWG proposes the establishment of a *Programme of Action for advancing responsible State behaviour in Cyberspace* with a view to ending the dual track discussions (GGE/OEWG) and establishing a permanent United Nations forum to consider the use of ICTs by States in the context of international security, taking into account the *acquis* of the previous GGEs and OEWG`s work in order to ensure a secure, stable, accessible and peaceful Cyberspace.

The positions expressed within OEWG are in perfect congruence with the concept of *global digital cooperation* proposed by the United Nations Secretary General in its 2019

Report The Age of Digital Interdependence [53] as referring to "ways of working together to address the societal, ethical, legal and economic impacts of digital technologies in order to maximise benefits to society and minimise harms" and as a means of exchanging knowledge and ideas. The approach of the UN in this regard is in accordance with the idea of an open Cyberspace and access to every person to this environment intended to be an inclusive digital economy and society [53].

All forms of rules proposed on cyber activities of States and international organizations-reports, statements or guides of best practices, codes of conduct, scholarly works are not binding and in a generic manner, all could be included in the category of *soft law* [54] or *quasi-norms* [55].

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*) [56] and does not involve the same legal remedies [57]. For example, as a general rule, a breach of an international obligation gives rise to reparations [58]. Applying this principle to cyberoperations, if a State`s cyber activity violates another`s State sovereignty, the State victim has the right to reparations [57], and this particular issue is still unclear.

Regulating Cyberspace appears to be in its beginning phase. In the future process of clarifying the content of rules applicable to States in Cyberspace the evolutive interpretation of existing norms and framework in this environment may prove useful. In this regard, it may be relevant the opinion of the International Court of Justice expressed in the *Advisory Opinion on Namibia*, which held that an

"international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of interpretation" [59].

and thus, taking into consideration the development of the legal system.

7 What is the meaning of normative equivalence?

Affirming the idea that the same rules and principles are applicable in the offline and online environment and to the same extent is a solution to solve the dilemma of an uncharted Cyberspace. However, it is not the complete solution and raises many questions and uncertainties as well, given the special features of this environment. As previously mentioned, the equivalence was promoted in the human rights field, as well, by several international bodies, jurisdictional and non-jurisdictional. Moreover, it was anticipated by international legal instruments providing that human rights and fundamental freedoms must be respected regardless of frontiers. This is the case of freedom of expression, enshrined in several universal and regional instruments that are legally binding or part of *soft law.* For example, Article 19 of the Universal Declaration of Human Rights provides that

*"*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media *and regardless of frontiers."*

The same terms – *regardless of frontiers* - are used by the International Covenant on Civil and Political Rights in its Article 19, the European Convention on Human Rights and Fundamental Freedoms in its Article 10, American Convention on Human Rights in its Article 13. Therefore, States have the obligation to respect freedom of expression in any environment, having a negative and a positive obligation at the same time [60].

Since 2012, the Human Rights Council stressed

"that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;" [61]

and at the same time

"2. Recognizes the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms;

3.Calls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries;"

The UN Human Rights Council reiterated these conclusions in 2014 [62].

Previously, the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue underlined the implications of the internet for the freedom of expression and access to information [63].

Also, at the universal level, UNESCO had an assiduous activity usually by cooperation with other entities in supporting Internet freedom and access to information and published a dedicated series on Internet Freedom, in connection with media freedom and pluralism [64]. These works are particularly relevant taking into consideration the moment they were adopted and divergent to the idea of applying cyber sovereignty as a form of control over the national territory. For example, *Declaration of Principles Building the Information Society: a global challenge in the new Millennium* [65], drafted in collaboration with the International Telecommunication Union highlights the importance of access to information for the information society and for the development of persons and society in its entirety.

Restrictions on the exercise of freedom of expression and access to information are admissible if they are in accordance with the requirements of the limitation clause provided by paragraph 3 of Article 19. The 2011 *General Comment no. 34* on freedom of expression of the Human Rights Committee [66] also underlines this conclusion in the following wording:

"Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."

Free access to Internet and digital networks without any barriers, technical, structural or educational is also supported by the OSCE [67]. The Council of Europe had the same approach of application of the same standards recognized for the offline environment to the online [68].

Not least, even the 2015 UNGGE Reports also expressly mention the respect of fundamental rights including the right to freedom of expression and the resolution and report adopted by the Human Rights Council and General Assembly [42]. As a consequence, there must be a balance between the admissible actions of States that constitutes interferences with the normal exercise of this right and its content. Establishing full state control over the infrastructure, flux of data and information as an effect of state cyber sovereignty would impact the right to access to information in a disproportionate and illegitimate way.

The general opinion on this issue determined the idea of fundamental digital rights [69] that actually show that the equivalence paradigm does not completely solve the problem on the framework applicable to human rights in Cyberspace. It is the same situation in respect of the rules and principles of International Law applicable in Cyberspace.

Scholars and works of different international bodies have revealed that the existing framework may not be completely adequate to address the complications determined by the special features of Cyberspace, especially in regard of human rights.

Exploring the efforts and works of different bodies within the United Nations clearly show that the challenges still exist and in time the topics to be addressed became more complex, which shows that a specialized approach is needed. At the moment, at the United Nations level, following the unsuccess of previous working groups, that are still active and they continue their mandate (in 2020, OEWG was renewed for the period 2021-2025 [70]) and, at the initiative of over 40 States, Programme of action on cybersecurity (PoA) was established; it will become a permanent mechanism after the 2021-2025 OEWG, more inclusive and will address comprehensively the issue of international norms in Cyberspace [71].

8 Conclusions

Applying the same normative framework to the online environment is clearly the best solution against considering the Cyberspace unregulated. However, the challenges posed by this environment that is continuously developing at a very rapid pace must be addressed and at the moment this is one of most sensitive topics of International Law. The normative equivalence must be also analysed through a critical lens which emphasizes the need for new human rights norms and implementation strategies specifically designed for application in cyberspace.

Further work from States and international bodies is needed to define the content, scope and limits of International Law principles and rules, by reference to those already established. The fact that different bodies within United Nations were not able to successfully develop International Law rules through diplomatic means and channels suggests this need and the inadequacy of the equivalence paradigm for this environment. Although its work and findings were incomplete and sometimes criticized, the United Nations continues to be the most appropriate and legitimate forum open to all States for discussing all types of issues related to cyberspace. Nevertheless, reaching a common view is more difficult but discussions and debates in the General Assembly would offer the premises of *opinio juris* on State behaviour and a global governance of Cyberspace.

All interests of multi stakeholders are interrelated and interconnected in Cyberspace. As an example, connected to International Law issues, the concept of cyber sovereignty, founded on the principle of sovereignty, is opposed to the idea of global governance of Cyberspace and does not take into account the interests of other stakeholders such as private companies and private persons, to whom Cyberspace is opened to. There is no obstacle in International Law in regulating Cyberspace and conduct of States and other stakeholders by reference to principles and rules already established that may be adapted to the special features of this environment. As it appears, state sovereignty in Cyberspace is limited and it does not have the same scope as the physical territory between its borders. The best approach in this regard would be taking into account that state sovereignty in Cyberspace relates to elements of physical infrastructure on which the existence of Cyberspace depends, yet the issues related to state jurisdiction and extra-territorial effects and what constitutes a breach of sovereignty in Cyberspace should be clarified.

Most States are silent and do not publicly express their position on how International Law applies. A possible interpretation is that they are reluctant to bind themselves to new rules until they are sure of how those rules will apply and how the technology and cyber environment will develop in the foreseeable future. Another possible interpretation is that silence provides the framework for any type of activity. This makes finding common ground on how International Law applies more difficult, but not an impossible task.

References

1. E. Donahoe, *The Need for a Paradigm Shift on Digital Security* in eds. F. O.Hampson, M. Sulmeyer, *Getting beyond Norms New Approaches to International Cyber Security Challenges Special Report*, Centre for International Governance Innovation, 31 (2017)
2. W. Gibson, Neuromancer (Ace Books, first published 1984)
3. J. Lillemose, M. Kryger, *Commentary Artikel på dansk, The (Re)invention of Cyberspace, Who invented cyberspace?,* URL: https://kunstkritikk.com/the-reinvention-of-cyberspace/, accessed 16.02.2023 (2015)
4. M. Baezner, P. Robin, *Trend Analysis: Cyber Sovereignty,* Risk and Resilience Team Center for Security Studies (CSS), ETH Zürich, 8 (2018)
5. R. Ottis, P. Lorents,. C*yberspace: Definition and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April, Reading: Academic Publishing Limited, 267-270, URL: https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/, accessed 16.02.2023 (2010)
6. Y. Shen, Chinese Political Science Review, **1:81**. 93, 82 (2016)
7. K. Nyman Metcalf, Tallinn Paper, **10**, 2 (2018)
8. D. Broeders, L. Adamson, R. Creemers, *Coalition of the unwilling? Chinese and Russian perspectives on cyberspace,* in The Hague Program For Cyber Norms Policy Brief, 2, URL: https://www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace, accessed 10.02.2023 (2019)
9. S. Arsène, *Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order?,* China Perspectives 2016/2 What Kind of International Order Does China Want, 28 (2016)
10. J. Zeng, T.Stevens, Y. Chen, Discourse of 'Internet Sovereignty', Politics & Policy, **45 (3)**, 432-464, 451 (2017)
11. M. Mueller, *Sovereignty and Cyberspace: Institutions and Internet governance,* Essay presented at the 5th Annual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana October 3rd 2018, URL: http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10410/5th-Ostrom-lecture-DLC.pdf?sequence=1&isAllowed=y, accessed 12.02.2023 (2018)
12. *Convention on Cybercrime*, 23.XI.2001, ETS No.185.
13. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Jan. 28, ETS No. 189 (2003)
14. Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security, 61st Plenary Meeting, Dec. 2 (2008)
15. Constitution and Convention of the International Telecommunication Union, Dec. 22, 1825 UNTS 330 (1992)
16. *The International Telecommunication Regulations* and their Appendices, adopted by the World Conference on International Telecommunications, Dubai, 2012/ International Telecommunication Union, Final Acts, of the World Conference on International Telecommunications (Dubai, 2012) (2013)

17. N. Pijović,. *The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms*, 13th International Conference on Cyber Conflict Going Viral, T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.) 2021NATO CCDCOE Publications, Tallinn, 215-231 (2021)
18. Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc A/69/723, URL: https://digitallibrary.un.org/record/786846?ln=en, accessed 12.02.2023
19. Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, Sixty-ninth session Agenda item 91 Developments in the field of information and telecommunications in the context of international security, A/69/723, URL: https://digitallibrary.un.org/record/786846?ln=en, accessed 12.02.2023
20. International Code of Conduct, para 1.
21. International Code of Conduct, para 2 (1).
22. D. Broeders, L.Adamson and R.Creemers (n 15) 2
23. M.N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, Cambridge, 2017)
24. F. Delerue, François, ESIL Reflections, **7:4**, 2 (2018)
25. E. Talbot Jensen, Georgetown Journal of International Law, **48**, 735-778 (2017)
26. *The Paris Call for Trust and Security in Cyberspace.* 2018, URL: https://pariscall.international/en/, accessed 12.02.2023
27. J. Guay, L. Rudnick, *What the Digital Geneva Convention means for the future of humanitarian action,* The Policy Lab June 25, URL: https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/, , accessed 12.02.2023 (2017)
28. V. Jeutner, Journal of International Humanitarian Legal Studies, **10 (1)**, 158–170 (2019)
29. M. Tolppa, O*verview of the UN OEWG developments: continuation of discussions on how International Law applies in cyberspace,* URL: https://ccdcoe.org/library/publications/overview-of-un-oewg-developments-continuation-of-discussions-on-how-international-law-applies-in-cyberspace/, accessed 10.02.2023 (2020)
30. CCDCOE. *Trends in International Law for cyberspace*, URL: https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf, accessed 12.02.2023 (2019)
31. S. Kanuck, Texas Law Review, **88**, 1575 (2010)
32. UNODA, *Fact Sheet - Developments in the field of information and telecommunications in the context of International Security*, URL: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf, accessed 12.02.2023 (2019)
33. I. J. van Os, *The United Nations, Global Cyberspace, and the Route to Hegemony,* Leiden University, URL: https://openaccess.leidenuniv.nl/bitstream/handle/1887/75333/Final%20Master%20Thesis%20GPE%202%20%281%29.pdf?sequence=1, accesssed 10.02.2023 (2019)

34. H. Moynihan, *Power Politics Could Impede Progress on Responsible Regulation of Cyberspace,* URL: https://www.chathamhouse.org/expert/comment/power-politics-could-impede-progress-responsible-regulation-cyberspace, accessed 10.02.2023 (2019)
35. UNODA, *Developments in the Field of Information and Telecommunications in the Context of International Security,* Fact Sheet, URL: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf, accessed 10.02.2023
36. M. Kaljurand, *United Nations Group of Governmental Experts: The Estonian Perspective*, in A.-M. Osula, H. Rõigas (eds.), *International Cyber Norms, Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn, 114, URL: https://dig.watch/processes/un-gge, accessed 10.02.2023 (2016)
37. UNGGE members in 2019-2021: Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, and Uruguay, URL: https://www.un.org/disarmament/group-of-governmental-experts/
38. United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 19, U.N. Doc. A/68/98, June 24, para 19, URL: http://undocs.org/A/68/98, accessed 10.02.2023 (2013)
39. A.-M. Osula, H. Rõigas, *Introduction*, in Anna-Maria Osula and Henry Rõigas (eds.), A.-M. Osula, H. Rõigas (eds.), *International Cyber Norms, Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn, 17, URL: https://dig.watch/processes/un-gge, accessed 10.02.2023 (2016)
40. United Nations, 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)
41. United Nations, *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, paras 20, 27, 28 (2013)
42. United Nations 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/70/174 (2015)
43. P. Meyer, *Norms of Responsible State Behaviour in Cyberspace*, in M.Christen, B. Gordijn, M. Loi (eds.), *The Ethics of Cybersecurity,* The International Library of Ethics, Law and Technology, **21**, 353 (2020)
44. E. Tikk, M. Kerttunen, Mika, *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, in Cyber Policy Institute, 14 (2017)
45. S. Soesanto, F. D'Incau,, *The UN GGE is dead: Time to fall forward. Commentary,* URL: https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance accessed 10.02.2023 (2017)
46. B. Lété, Bruno, P. Chase, Peter, *Shaping Responsible State Behavior in Cyberspace*, in The German Marshall Fund of the United States Workshop Briefing Paper, 6 (2018)
47. UN General Assembly, General Assembly*, Developments in the field of information and telecommunications in the context of international security*, UN Doc A/RES/73/27, URL: https://undocs.org/A/RES/73/27, accesed 10.02.2023 (2018)

48. UN General Assembly General Assembly, *Resolution adopted by by the General Assembly on 22 December 2018 on Advancing responsible State behaviour in Cyberspacein the context of international security*, UN Doc A/RES/73/266, URL: https://undocs.org/en/A/RES/73/266, accessed 10.02.2023 (2018)
49. UN GGE Chair`s Summary, URL: https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf. accessed 10.02.2023 (2019)
50. T. Maurer, Hague Journal on the Rule of Law,**12**, 283–305 (2020)
51. Statements by the Republic of Finland Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security Virtual Informal Consultations 19 June and 2 July 2020, Statement 2 delivered 2 July 2020, URL: https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-finland-19-june-and-2-july-2020.pdf, accessed 10.02.2023
52. *The future of discussions on ICTs and Cyberspace at the UN,* URL: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf, accessed 10.02.2023 (2020)
53. United Nations High-Level Panel on Digital Cooperation, *The Age of Digital Interdependence*, *Report of the UN Secretary-General's High-level Panel on Digital Cooperation*, URL: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf, accessed 09.02.2023 (2019)
54. D. Shekton, *International Law and 'Relative Normativity*', in ed. M. D. Evans, International Law, Fourth Edition. 159 (Oxford Universrity Press, Oxford, 2014)
55. T. Erskine, M. Carr, *Beyond 'Quasi-Norms: The Challenges and Potential of Engaging with Norms in Cyberspace*', in A.-M. Osula, H. Rõigas (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, 100 (NATO CCDCOE Publications, 2016)
56. International Law Commission. 2001, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, by the Commission at its fifty-third session, in 2001, and submitted to the General Assembly as a part of the Commission's report covering the work of that session, annex to General Assembly resolution 56/83 of 12 December 2001, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf, accessed 09.02.2023
57. M. N. Schmitt, L. Vihul, *The Nature of International Law Cyber Norms*, Tallinn Paper No. 5 Special Expanded Issue, 31, URL:https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-5-Schmitt-and-Vihul.pdf. accessed 10.02.2023 (2014)
58. Cour permanente de Justice internationale, *Chorzow Factory Case*, 1928 PCIJ., (ser. A) No. 13, at 28.
59. International Court of Justice, Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276,Advisory Opinion, I.C.J. Reports 1971, 16. para 53 (1970)
60. G. Rona, Gabor, L. Aarons, Journal of National Security Law & Policy, **8:503**, 505-506 (2016)
61. Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, United Nations A/HRC/20/L.13, 29 June (2012)
62. United Nations General Assembly, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/26/13 26/13, URL: https://documents-dds-

ny.un.org/doc/UNDOC/GEN/G14/082/83/PDF/G1408283.pdf?OpenElement, accessed 10.02.2023 (2013)

63. Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, A/HRC/17/27, URL: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, accessed 10.02.2023 (2011)
64. UNESCO, URL: https://www.unesco.org/en/freedom-expression-online, accessed 10.02.2023 (2022)
65. World Summit on the Information Society Geneva 2003-Tunis 2005,WSIS-03/GENEVA/DOC/4-E, 12 December, URL: https://www.itu.int/net/wsis/docs/geneva/official/dop.html, accessed 20.02.2023 (2005)
66. Human Rights Committee, *General comment No. 34, Article 19: Freedoms of opinion and expression*, CCPR/C/GC/34 July 2011, para 43 (2011)
67. Organization for Security and Co-operation in Europe, *The Representative on Freedom of the Media Amsterdam Recommendations, Freedom of the Media and the Internet,* URL: https://www.osce.org/files/f/documents/4/a/41903.pdf, accessed 12.02.2023 (2003)
68. Council of Europe, Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies), URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44, accessed 10.02.2023 (2016)
69. D. Dror-Shpoliansky, Y. Shany, EJIL, **32(4)**, 1249–1282, DOI: 10.1093/ejil/chab087 (2021)
70. United Nations General Assembly, *Developments in the field of information and telecommunications in the context of international security*, Resolution adopted by the General Assembly on 31 December 2020, A/RES/75/240, URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf?OpenElement, accessed 12.02.2023 (2021)
71. United Nations General Assembly, *Developments in the field of information and telecommunications in the context of international security*, Resolution adopted by the General Assembly on 7 December 2022, A/RES/77/37, URL: https://digitallibrary.un.org/record/3991743?ln=en, accessed 10.02.2023 (2022)