Legal Issues in the Digital Age. 2022. Vol. 3, no. 1.
Вопросы права в цифровую эпоху. 2022. Т. 3 № 1.

Research article
УДК: 341
DOI:10.17323/2713-2749.2022.1.61.80

Standard-setting and Normativity in International Governance of Interstate Relations in the Information and Communication Technologies Context

Vera Nikolayevna Rusinova

National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Moscow 101000, Russia, vrusinova@hse.ru, ORCID: 0000-0002-5838-0283

Abstract

The paper considers how the standard-setting path, taken by states with respect of the information and communication technologies (hereinafter: ICTs), correlates with the normativity in international governance of this sphere. The pro-normative reading of this question pushes to examine whether this path designates a pre-lawmaking phase, contributes to the interpretation of the *lex lata* general norms, or fills in the gaps that cannot be covered by the orthodox international lawmaking. The counter-normative reading assesses whether the standard-setting path precludes, contests, freezes, or substitutes the lawmaking. In order to fulfill these tasks, the author concentrates on two standard-setting sources: the 'non-binding norms, rules, and principles of responsible state behaviour' adopted by the UN level in relation to ICTs related context and International Code of Conduct for Information Security, drafted by the states–members of the Shanghai Cooperation Organization. The paper reveals that 'non-binding norms, rules, and principles' elaborated at the UN level do not change the scope of binding provisions of International law. Thus, the content of these standards did not generate any 'added value' with respect to the negative and positive obligations of the states. Moreover, these standards cannot serve as an interpretation or understanding as to how existing international law applies to ICTs precisely because of the caveat made by the states with respect to the additional, subordinated role of these norms, rules, and principles. Such constellation puts in place a 'normative

gap scenario' showcasing that for the many states the legal uncertainty and legal gaps are a more profitable constellation. However, should the states follow the standard-setting track and adhere to the non-binding norms, provided that they are relaxing existing legal obligations of states, this 'deviation scenario' will also erode the normativity of International law. A solution can be found in the stage-by-stage shift from the standard-setting to the law-creating track. Already elaborated norms, rules, and principles of responsible state behaviour allow this shift for. It can happen in two stages: at the level of content and then with respect to the nature of these norms.

Keywords

standards; information and communication technologies (ICTs); International Law; normativity; responsible state behaviour.

***For citation*:** Rusinova V.N. (2022) Standard-setting and Normativity in International Governance of Interstate Relations in the Information and Communication Technologies Context. *Legal Issues in the Digital Age,* vol. 3, no. 1, pp. 61–80. DOI:10.17323/2713-2749.2022.1.61.80

Introduction

Cyber security has started to gain more weight in the international political agenda at the universal, regional, and bilateral levels since 1998[1]. This agenda had a very clear-cut legal segment. From the very beginning, both governmental and academic discourse surrounding the application of International law to information and telecommunication technologies (hereinafter: ICTs) was put and nurtured in the 'whether and how' ontological frame. A designation of forms of possible legal contribution were confined to interventionist (managerial) and lawmaking actions [D'Aspremont J., 2016: 577–579, 582–583]. According to this binary, the current stage of legal affairs drifts between two dimensions, namely an acknowledgment of applicability of International law and precision of the existing and non-cyberspecific legal norms. The former culminated in the Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security (hereinafter: the GGE) reports of 2015 and 2021, thus, serving as a response to the 'whether'-question. The latter

[1] Resolution of the UN General Assembly. 4 December 1998. A/RES/53/70. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement (accessed: 15.02.2022

adopted the form of individual interpretation by states on the one hand[2] and their collective elaboration of the standards on the other hand, addressing the 'how'-question.

The standard-setting initiatives in all possible formats, including governmental, hybrid, corporate, and academic are continuing to boom. At the UN level, states concentrated on operationalization of the 'norms, rules, and principles of responsible state behaviour' in relation to ICT, capacity- and confidence-building measures. This work started in the GGE and was fleshed out in 2015 report[3], continued in 2019-2021 in parallel in the

[2] Australia: Department of Foreign Affairs and Trade. Australia's Cyber Engagement Strategy. Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace. 2019. Available at: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF (accessed: 08.11.2021); Australia's Cyber Engagement Strategy. Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace. 2017. Available at: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20 Strategy.pdf (accessed date: 08.11.2021) (далее — Australia's Cyber Engagement Strategies); United Kingdom: Cyber and International Law in the 21st Century. Attorney General Jeremy Wright Speech on the UK's Position on Applying International Law to Cyberspace; Mission to the United Nations: UK Statement on the Application of International Law to States' Conduct in Cyberspace, para 10. June 3, 2021. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990851/ (accessed: 10.02.2022); application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.pdf; the Netherlands: Ministry of Foreign Affairs. Letter to the Parliament on the International Legal Order in Cyberspace. 5 July 2019. Available at: https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace (accessed: 08.11.2021); Finland's National Positions, International Law and Cyberspace. 2020. Available at: https://front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyber-and-international-law-oct-2020.pdf (accessed: 28.01.2022); France. Ministère des Armées. International Law Applied to Operations in Cyberspace. October 2019. Available at: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (accessed: 26.11.2021); Germany. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. A.S. Neu, A. Hunko, W. Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE. Krieg im 'Cyber-Raum' — offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung. Drucksache 18/6989. 10.12.2015. S. 4, 5–7. Available at: https://dserver.bundestag.de/btd/18/069/1806989.pdf (accessed: 17.01.2022); US: [Koh H.: 2012]; nine Latin American states: [Hollis D., 2020: 5]. See also: Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266 (A/76/136). Available at: https://www.un.org/disarmament/group-of-governmental-experts/ (accessed: 12.02.2022)

[3] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Report (June 26, 2015).

GGE and the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter: OEWG)[4], and since that time has been carried out by the latter[5]. In 2011, a group of states led by Russia and China has promoted the submission of the International Code of Conduct for Information Security to the UN (known as the SCO[6] Code of Conduct), and presented an updated version in 2015[7]. Hybrid standard-setting initiatives embrace the 2018 Paris Call for Trust and Security in Cyberspace proposed by France, which was endorsed by 81 states, the EU, and more than 700 companies[8]. The 2018 Charter of Trust, which contained ten principles of cyber security was initiated by Siemens in partnership with the Munich Security Conference. The Charter was primarily designated for private sector companies, however it was endorsed by the German Federal Office for Information Security[9]. The 'six critical norms' ('Singapore norms package') was proposed in 2018 by the multi-stakeholder group called the Global Commission on the Stability of

A/70/174. [hereinafter: GGE Report 2015]. Available at: https://undocs.org/A/70/174 (accessed: 15.02.2022)

[4] Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. 14 July 2021. A/76/135 [hereinafter GGE Report 2021]. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement (accessed: 15.03.2022); Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Final Substantive Report. 10 March 2021. A/AC.290/2021/CRP.2. Available at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed: 12.02.2022)

[5] Resolution of the General Assembly. 31 December 2020. A/RES/75/240. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf?OpenElement (accessed: 12.02.2022)

[6] The Shanghai Cooperation Organization.

[7] International Code of Conduct for Information Security, Annex to the letter of 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. Available at: https://digitallibrary.un.org/record/710973?ln=en (accessed: 14.01.2022); International Code of Conduct for Information Security. Annex to the letter of 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. A/69/723. Available at: https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf (accessed: 15.02.2022)

[8] Available at: https://pariscall.international/en/ (accessed: 12.02.2022)

[9] Available at: https://press.siemens.com/global/en/feature/charter-trust-takes-major-step-forward-advance-cybersecurity#:~:text=At%20the%20Munich%20Security%20Conference,cybersecurity%20and%20further%20advance%20digitalization (accessed: 12.02.2022)

Cyberspace[10]. In 2016, the Freedom Online Coalition issued Recommendations for Human Rights Based Approaches to cybersecurity[11]. There are also a number of private initiatives, for instance the Microsoft's Cybersecurity Tech Accord[12], supported by about 150 IT companies and a voluntary set of good practices to improve routing security entitled the Mutually Agreed Norms for Routing Security (MANRS). This initiative was joined by network operators, Internet Exchange Points, CDN and cloud providers, and equipment vendors[13]. The most prominent academic standard-setting initiative is the Oxford Process on International Law Protections in Cyberspace that embraces a number of recommendations dedicated to different types of the ICTs operations[14]. Alongside with the taxonomy of standards drawn on their respective authors, the emergence of a form of standard setting falling outside the orthodox legal and political instruments should be also noted. Namely, the regulation by design, which is carried out by a technical language of algorithms and programming, i.e., 'design-based regulation embeds standards into design at the standard-setting stage in order to foster social outcomes deemed desirable' [Yeung K., 2017: 120].

At the same time, the creation of legally binding norms in the cyber sphere is not at an absolute standstill, but three aspects render these processes to have a limited impact. Firstly, the scope of this international lawmaking, as a rule, does not cover the substantial issues related to the legality of the interstate cyber interferences. Instead, a growing mass of treaty provisions have been focused on criminalization of cybercrimes and related to jurisdictional and procedural matters[15], or information sharing

[10] Available at: https://cyberstability.org/?news_category=norm-proposal (accessed: 12.02.2022). The Group was founded in 2017 and concluded its activities in 2021.

[11] Available at: https://freedomonlinecoalition.com/wg1-launches-recommendations-on-human-rights-based-approaches-to-cybersecurity/ (accessed: 12.02.2022)

[12] Available at: https://cybertechaccord.org/accord/ (accessed: 12.02.2022)

[13] Available at: https://www.manrs.org/ (accessed: 12.02.2022)

[14] Available at: https://www.elac.ox.ac.uk/the-oxford-process/ (accessed: 01.02.2022)

[15] The first and oldest treaty, the 2001 Budapest Convention on Cybercrime, that seeks to harmonize substantive, procedural and jurisdictional legal issues on cybercrimes, has long overspepped the status of a regional international treaty. Under the autspicies of the League of Arab States all its states members have signed and — except for Saudi Arabia — ratified the 2010 Convention on Combating Information Technology Offences which aims to strengthen cooperation between the Arab States and repeats the model for co-operation set by the Budapest convention. The 2014 African Union Convention on Cyber Security and Personal Data Protection, that have a more extensive material scope, governing not only cyber security, but also electronic transactions and personal data protection, has not entered into force yet, having collected only five ratification so far (whilst 15 are needed).

and capacity building[16]. Secondly, a few lawmaking projects embracing binding rules, relevant for legal qualification of the interstate operations, though having resulted in the international treaties that have entered in force, are entirely regional initiatives driven by Russia in the Commonwealth of Independent States (hereinafter: CIS) and the Collective Security Treaty Organization (hereinafter: CSTO)[17], or jointly by Russia and China in the framework of the Shanghai Cooperation Organization (hereinafter: SCO) [Zinovieva E., 2019]. Thirdly, the sole initiative at the universal level is an elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, which will cover the criminalisation of the ICTs-related malicious behaviour and cooperation on matters of criminal procedure only[18].

The aim of this paper is to consider how this standard-setting path, taken by states, correlates with the normativity in international governance of information and communication technologies. The pro-normative reading of this question will be to examine whether this path designates a pre-lawmaking phase, contributes to the interpretation of the *lex lata* general norms, or fills in the gaps that cannot be covered by the orthodox international lawmaking? The counter-normative reading assesses whether the standard-setting path precludes, contests, freezes, or substitutes the lawmaking?

---

[16] For example, see: Directive (EU) 2016/1148 of the European Parliament and of the Council Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. 6 July 2016 // Official Journal of the European Union. L 194/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN (accessed: 1.02.2022)

[17] The 2009 Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO. Bulletin of International Treaties. № 1. 2012. Available at: http://eng.sectsco.org/load/207508/ (accessed: 1.02.2022). The 2013 Agreement on Co-operation of the States Members of the Commonwealth of Independent States in the Field of Ensuring Information Security (20 November 2013). Bulletin of International Treaties. № 10. 2015. Available in Russian at: URL: https://base.garant.ru/70604710/ (accessed: 01.02.2022); The Agreement of the States Parties of the Collective Security Treaty Organization in the Field of Ensuring Informational security. 30 November 2017. Available at: URL: http://publication.pravo.gov.ru/Document/View/0001201904260001 (accessed: 12.02.2022)

[18] Resolution adopted by the General Assembly, Countering the use of information and communications technologies for criminal purposes (26 May 2021). A/RES/75/282. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement (accessed: 1.02.2022)

1. 'Norms, Rules, and Principles of Responsible State Behaviour' Elaborated Under the United Nations Umbrella

1.1. The Advent of the Standard-Setting Track

The setting of standards, which are called 'non-binding norms, rules, and principles of responsible state behaviour', is a clear-cut contemporary trend and track chosen by the states as a response to the necessity to determine the 'rules of the game' in the ICTs relations. This conclusion follows from the results of the previous UN GGE work, which culminated in the acknowledgment of general applicability of International law to ICTs and the elaboration of 11 substantial standards[19], which were endorsed by the UN General Assembly resolutions adopted by consensus[20]. In 2018, the same body supported the standard-setting track and using a majority vote added two new norms to the initial list of the GGE[21].

The choice of the standard-setting track was also confirmed by the states' delegations at the two substantial sessions of the Open-Ended Working Group[22], established by the UN General Assembly in parallel with a new GGE in 2019-2020[23]. The overwhelming majority of states explicitly preferred not to create any new legally binding instruments. Explicitly articulated grounds for this had references to the sufficiency of the current 'strategic framework'[24] for regulation of the cyber sphere. Another reason included the danger that the creation of new legally binding instruments will undermine or create uncertainty in respect to the existing ones[25]. Fi-

[19] GGE Report 2015.

[20] UN General Assembly Resolution. Developments in the field of information and telecommunications in the context of international security. 23 December 2015. A/RES/70/237. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/57/PDF/N1545757.pdf?OpenElement (accessed: 1.02.2022)

[21] UN General Assembly Resolution. Developments in the field of information and telecommunications in the context of international security. 5 December 2018. A/RES/73/27. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement (accessed: 10.02.2022)

[22] Ibid.

[23] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report. 10 March 2021. A/AC.290/2021/CRP.2, para 24-33. Available at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed: 10.02.2022)

[24] EU statement at the 1st subs. session of the OEWG, 9–12 September 2019 (Portugal joined). Available at: http://webtv.un.org/ (accessed: 1.11.2021)

[25] Bulgaria and Italy at the 1st subs. session of the OEWG.

nally, a lack of consensus among states[26] or a lengthy nature of international lawmaking, which contrasts with the speed of technological developments were brought to the fore[27]. Only a minority of states favoured a necessity of lawmaking[28]; some of them did so with a reservation that they consider a development of new binding norms as a medium or long-term objective[29]. The preference of the standard-setting track was enhanced by a strong consensus on the need to concentrate on strengthening awareness, operationalization, and implementation of the GGE recommendations and development of capacity building. Finally, the priority of the five-years mandate of a new (the second) OEWG is to continue to further develop 'the norms, rules and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour'.

1.2. The Content and Significance of the GGE Non-binding Norms, Rules and Principles of Responsible State Behaviour

Analysing different impacts that the standard-setting track may have for the normativity of International law implies a necessity to dwell on the content of these non-binding norms of responsible state behaviour. It is worth examining how these norms relate to the existing non-cyberspecific provisions of International law, and then subject a subsequent qualification of the forms of the states' behaviour towards these standards to the results of this content-based analysis. The GGE Report of 2015 contains 11 'norms, rules and principles for the responsible behaviour of states'. The Endorsement of these standards gained consensus of the UN General Assembly[30] and their content was not disputed at the substantial meetings of the OEWG in 2019–2020.

As it is clarified by the GGE, these 'norms do not seek to limit or prohibit action that is otherwise consistent with international law'[31], so 'norms

[26] Israel and UK at the 1st subs. session of the OEWG.

[27] The US, Chile, Australia, Japan at the 1st subs. session of the OEWG. 2019; Singapur, UK, Australia at the 2nd subs. session of the OEWG. 10–14 February 2020. Available at: webtv.un.org (accessed: 7.11.2021)

[28] A necessity of lawmaking was expressed by the CARICOM group, Algeria, Nigeria, Syria, Russia, India, China, Malasia, Indonesia, Singapur, and Jordan.

[29] South Africa and Chile at the 1st subs. session of the OEWG; Brazil, joined by Pakistan, Cuba and Egypt at the 2nd subst. session of the OEWG.

[30] Resolution adopted by the General Assembly. 23 December 2015. A/RES/70/237, para 2 (a).

[31] GGE Report 2015, para 10.

and existing international law sit alongside each other'[32]. The OEWG also stressed that 'norms do not replace or alter states' obligations or rights under international law, which are binding' as they provide 'additional specific guidance on what constitutes responsible state behaviour in the use of ICTs'. Thus, it was not the intention of the states to reduce or change the existing *lex lata* rules of international law and challenge their normativity [Akande D., Coco A., Dias T., 2022: 31].

However, the content of these recommendations is different: some of them do reflect, repeat or can be deduced from the existing international obligations. For instance, this is true for the obligation to cooperate, respect of human rights, the obligation not to conduct and not to knowingly support ICT activity contrary to the states' obligations under international law. Some, as for instance the cyber due diligence obligations, have a weaker basis in International law. As the UK Mission to the United Nations stated, 'the fact that States have referred to this [cyber due diligence] as a non-binding norm indicates that currently there is no State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace'[33]. A legal obligation of 'cyber due diligence', requiring states to ensure that 'their territory is not used as a base for state or non-state hostile cyber operations against another state that cause serious adverse consequences with regard to a right of the target state' [Schmitt M.T., 2017: 30-50], exceeds a general duty of the states 'not to allow knowingly its territory to be used for acts contrary to the rights of other States'[34]. This concept is still in a nascent form and, despite the positions of some states[35] and the existence of a 'patchwork' of already existing

[32] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (A/76/135). 14 July 2021, para 15. Available at: https://www.un.org/disarmament/group-of-governmental-experts/ (accessed: 12.02.2022)

[33] UK. Mission to the United Nations, UK. Statement on the Application of International Law To States' Conduct in Cyberspace. June 3, 2021, para 10. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990851/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.pdf (accessed: 12.02.2022)

[34] Corfu Channel Case (UK v. Albania). Judgment .9 April 1949. I.C.J. Reports. 1949. P. 4.

[35] The Netherlands: Ministry of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace, pp. 4-5. July 5, 2019. Available at: https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace; France: Ministère des Armées, International Law Applied to Operations in Cyberspace 2019. Available at: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (accessed: 15.02.2022)

general due diligence duties' [Dias T., Coco A., 2022: 198] is widely considered *lex ferenda* [Shackelford S.J., Russell S., Kuehn A., 2016: 22-23].[36] Finally, some norms, rules, and principles of responsible state behaviour are not underpinned by the existing legally binding rules of international law. They constitute political commitments or 'soft law' arrangements.

By their content, these norms, rules, and principles of responsible state behaviour do not alter the nature of binding provisions of International law, mainly because of two safeguards. The first one lies in the design of formulations. Standards that may be relevant for setting the contours of the outlawed cyber activities are constrained by references to *lex lata* International law. For instance, the first obligation to cooperate in developing and applying relevant measures and preventing malicious ICT practices is subjected to the 'purposes of the United Nations'[37]. The third norm prohibits states to allow to use their territory for using ICT only if it constitutes an 'internationally wrongful act', which serves as a clear mentioning of the existing binding norms of International law[38]. The fifth norm is reiterating that 'the same rights that people have offline must also be protected online' by an explicit reference to the UN Human Rights Council and General Assembly resolutions, which, in turn, are based on the International Covenant on Civil and Political Rights[39]. A promising sixth norm, which could have significantly contributed to the outlawing of state-on-state cyber-operations should it be limited to state activity that 'intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public', remarkably confines the scope of this prohibition to the activities violating their obligations under International law[40].

The second umbrella safeguard envisaged in the 2015 GGE report provides for that these 'norms do not seek to limit or prohibit action that is

[36] The GGE Report 2015 at 13 (3) envisages a negative obligation of states 'not knowingly allow their territory to be used for internationally wrongful acts using ICTs' as one of the 'voluntary, non-binding norms, rules or principles of responsible behaviour of States'. See U.S. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. 10 May 2011. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; (accessed: 16.11.2020)

[37] GGE Report 2015, para. 13 (a).

[38] Ibid, para 13 (c); UN General Assembly Resolution. 12 December 2001. Responsibility of States for Internationally Wrongful Acts. A/RES/56/83. Art. 1-2. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/477/97/PDF/N0147797.pdf?OpenElement (accessed: 12.02.2022)

[39] GGE Report 2015, para 13 (e).

[40] Ibid, para 13 (f).

otherwise consistent with international law'[41]. During substantial meetings of the OEWG, many states also underscored that the standards do not replace the existing international obligations of states[42]. The OEWG report also reiterates the same approach that norms 'rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs'[43].

The UN General Assembly added two new norms to the list and altered few aspects in the GGE formulations in the resolution on the establishment of the OEWG in 2018[44]. However, it was adopted by voting and not by consensus with 119 votes in favour, 46 against, and 14 abstentions[45]. In any case, the novelties introduced by this resolution, according to their content, do not touch upon the scope of the states' negative obligations, even when taking into account the absence of the general disclaimer on conformity of norms with legally binding rules (in contrast to the 2015 GGE Report). New norms reflected in this resolution are dedicated to the exchange of information, prevention of proliferation of malicious ICT tools, and broadening of the scope of actors involved in the relevant discourses[46]. Notably, in its 2021 report, the GGE commented on the initial list consisting of 11-non-binding norms, and not on an extended one[47].

Thus, the content of the standards both in its initial and extended versions did not generate any 'added value' with respect to the negative obligations of the states[48]. The opinion, expressed by D. Akande, A. Coco and T. Dias, who argued that these norms, rules, and principles 'are not deprived of any legal significance as they lay out possible, timely, and widely accept-

[41] Ibid, para 10.

[42] Netherlands, 1st subst. meeting, 2019.

[43] Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 2020. P. 7. Available at: https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf (accessed: 15.02.2022)

[44] UN General Assembly Resolution. Developments in the field of information and telecommunications in the context of international security.5 December 2018. A/RES/73/27. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement (accessed: 15.02.2022)

[45] Available at: https://www.un.org/press/en/2018/ga12099.doc.htm (accessed: 15.02.2022)

[46] The UN General Assembly Resolution. A/RES/73/27, para 1.4, 1.10, 1.13.

[47] GGE report 2021, para 15–68.

[48] Against this background it is revealing that during the OEWG sessions in 2019–2020 only Egypt explicitly suggested transforming the recommendations of the GGE to legally binging, and Phillipines expressed concern about non-binding their nature and reduced options for complaence and enforcement.

ed interpretations or understandings as to how existing international law applies to ICTs' [Akande D., Coco A., Dias T., 2022: 35] contrasts with the general rule of interpretation. According to Art. 31 (3) (a) of the Vienna Convention on the Law of Treaties[49], which is widely regarded as a reflection of the customary law applicable to both treaty and customary norms, 'any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions' should be taken into account together with the context of the treaty. As no formal requirements are set forth for these 'agreements', the GGE reports adopted by a consensus and the General Assembly resolutions listing the recommendations on the respectful behaviour in the ICTs context, especially taking into account those that were adopted without a vote, can fall under this category. However, the caveat made by the states with respect to the additional, not substitutional role of these 'norms, rules, and principles' does not allow them to be used as means of interpretation of the existing treaty and customary law. They are, consequently, not exceeding the frame of the non-binding recommendations.

This standard-setting track may be important and justified as a political instrument to reaffirm the applicability of International law to cyber specific interstate relations. However, by its content, it is legally tautological in the sense that it does not change anything in the assessment of the legality of interstate cyberoperations. It cannot be said that the states did not notice this fact: a necessity to change or add these norms was discussed at the OEWG sessions. However, whilst the need to concentrate on implementation and operationalisation of these norms met general acceptance, only twelve states insisted on development of this list[50]. Argentina, Brazil, Egypt, Finland, France, Germany, the Netherlands, Pakistan, Singapore, Sweden, and the UK suggested to add norms dedicated to the protection of the public segment of the Internet and electoral infrastructure[51]. China proposed further ensuring the integrity of the ICT supply chain, namely that states should not exploit their dominant positions to undermine the supply chain security of ICT goods and services of other states[52]. The ICRC

[49] Vienna Convention on the Law of Treaties.23 May 1969. United Nations. Treaty Series. Vol. 1155. P. 331.

[50] The Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. 2nd session of the OEWG. 11 February 2020. Available at: webtv.un.org (accessed: 07.11.2021)

[51] 2nd subst. session of the OEWG (Norms, Rules and Principles) 10 February 2020. The UK expressed concerns on the concept of the public core of the Internet.

[52] 1st subst. session of the OEWG, 6th meeting. Available at: https://dig.watch/resources/6th-meeting-first-substantive-session-open-ended-working-group-oewg

represented additional norms protecting the medical facilities[53]. The limitation of the mandate and the lack of consensus did not allow the OEWG to include any of the proposed norms in the recommendations forwarded to the consideration of the General Assembly[54]. This fact puts in place a 'normative gap scenario' showcasing that for the majority of states the uncertainty and legal gaps are a more profitable constellation despite their double-edge nature. As a result, the states are not additionally bound by the political or legal obligations.

Two opposing stances framing the problematique of the necessity of new binding rules restricting states' sponsored cyber operations are an appeal to the necessity of law as a system able to restrict, deter, and enable the use of the tools of international responsibility. This view is based on the normativity of International law. In the other corner of continuum is a realistic vision of a deterrent role of the offensive cyber-capacities and a wide possibility for tit-for-tat, which is slightly limited by *lex lata* international legal provisions. During the OEWG sessions this — otherwise implicit — binary was strikingly incarnated in an initiative to introduce a general obligation to refrain from the weaponization and offensive uses of ICTs. This motion, proposed by Cuba, Indonesia, India, Iran, Nigeria, and Pakistan, triggered an immediate objection from Australia, Denmark, and the UK. They insisted on a necessity to respect the existing limitations of the usage, but not the outlawing of the possession or development of offensive cyber capabilities[55]. These stances are not as different as it might seem. States insisting on a need for additional norms in the form of standards meant political, and not legal commitments. Even if the proposals should have dealt with the binding rules, the nature of the normative force of International law cannot be exhaustively explained by a purely formalistic approach [D'Aspremont J., 2011]. States cherishing the under inclusiveness of the *lex lata* provisions are not really contesting the normativity of International law, not only because whilst declining to elaborate new legally binding norms, they claim to obey the existing rules, but also because their actions are driven by the presumption that these new norms will have normative force and limit their behaviour.

(accessed: 20.06.2020). This proposal was also envisaged in the SCO Draft Code and supported at the first OEWG sessions by Russia (2nd subs. session, 10 February.2020).

[53] 2nd subst. session of the OEWG… 10 February 2020.

[54] The OEWG Final Substantive Report. 10 March 2021. A/AC.290/2021/CRP.2. Available at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed: 0 8.11.2021)

[55] 2nd subst. session of the OEWG…10 February 2020.

A solution can be found in the stage-by-stage shift from the standard-setting to the law-creating track. Already elaborated norms, rules, and principles of responsible state behaviour allow this shift for, provided that the above-mentioned safeguards will be lifted. It can happen in two stages: at the level of content and then with respect to the nature of these norms.

2. The International Code of Conduct for Information Security

2.1. The content of the Code

The group of SCO states consisting of the former USSR republics, i.e, the Russian Federation, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan plus China sponsored the initiative to adopt the International Code of Conduct for Information Security. The draft was initially submitted to the UN General Assembly in 2011 and a revised version was filed in 2015[56]. Both drafts were composed in the form of a potential General Assembly resolution and sought to achieve 'earliest possible consensus' on the issue of 'information security'. The text of the Code consists of very general provisions and constitutes rather a list of goals and principles, than a draft of concrete norms. Nonetheless, what matters is the stance taken by the states sponsoring this Code in respect of the already existing legal framework.

According to the preamble of the revised version of the Code, the drafters took as a starting point the availability of norms 'derived from existing international law', which are applicable to the use of ICTs by states, and pledged to a necessity to form a consensus on how these norms can be applied in this context[57]. At the same time, they acknowledged that additional norms 'can be developed over time', making a reference to para. 16 of the Report of the GGE, which contains a list of voluntary confidence-building measures[58]. By their content, the provisions of the Code can be classified into several categories. The first one comprises the repetition of already existing principles of International law, such as to comply with the UN Charter, respect sovereignty, territorial integrity, and political independence of all states, respect human rights, peacefully settle the disputes, refrain

[56] International Code of Conduct for Information Security. Annex to the letter 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. A/69/723 (hereinafter: SCO Code 2015).

[57] Ibid, para 9.

[58] GGE Report 2015, para 16.

from the use of force, and cooperate[59]. The obligation to respect rights and freedoms in the information space fully repeats provisions of Art. 19 of the ICCPR. Only a duty not to interfere in internal affairs of other states is formulated in a scope that goes beyond the existing two-elements test, i.e., interference to the *domaine réservé* and a coercive character[60]. In particular, the Code not only provided that only one element is enough, but also broadened of the second category to include the undermining of stability[61]. A pledge not to carry out activities which run 'counter to the task of maintaining international peace and security'[62], should this general aim be interpreted in light of the UN Charter, can be also qualified as making no difference in comparison to the existing legal framework. Almost the same is true for the legal protection of information space and critical information infrastructure.

The 2015 Code, besides some stylistic upgrades, delivers only two novelties, both of which are designed to challenge the existing multistakeholder model of Internet governance. The first one is a pledge to supply 'chain security' in order to prevent other states from 'exploiting their dominant position' to undermine the states' 'right to independent control' of relevant goods and services or to threaten their security[63]. The second novelty is a call for equality of states in international governance of the Internet[64]. In comparison to the previous version, the updated one does not contain a definition of an 'information weapon' and does not use the phrase 'proliferation of information weapons'. However, the foreign commentators were sceptical about the prospects of the revised version, for 'the new wording is consistently very broad, allowing that any use of 'information and communications technologies' could be qualified as inconsistent with 'maintaining international peace and security' [Rõigas H., 2015].

2.2. Impact of the Code

Both initial and revisited drafts were disseminated by the UN Secretary General and although drafted in the form of a General Assembly resolution, they were not discussed at the sessions of this UN body. Although the

[59] SCO Code 2015, para 1, 4, 7, 12, 13.

[60] ICJ. Case concerning Military and Paramilitary Activities in and against Nicaragua, Nicaragua v. United States of America. Judgment of 27 June 1986. I.C.J. Reports. 1986. P. 14. § 205.

[61] SCO Code 2015, para 3.

[62] Ibid, para 2.

[63] Ibid, para 5.

[64] Ibid, para 8.

influence of the Code can be tracked at the UN level, its impact was rather very modest. References to these drafts can be found in the GGE reports[65], however, they were not followed by the application of the content[66]. The language of the Code was initially introduced in the draft of the General Assembly resolution in 2018, but was removed from the final version[67].

As for the position of other states, only United States has explicitly expressed its negative position. In 2012, the Congress has adopted a resolution,[68] criticising the Code for challenging the existing multi-stakeholder model of Internet governance and reserving a position for the US representative to oppose, should the UN or any other international organization vote for the Code. The reaction of the 'western' scholarship was also harsh and concentrated on the threat of the advancement of censorship, an attempt to overlay territorial sovereignty on the Internet [Mueller M., 2011]; [Carr J., 2011]; [Segal A., 2012] and a very broad approach to ICTs, which could be classified as inconsistent with 'maintaining international peace and security'. The next critique was related to the human rights restrictions mentioned in the revised Code. This interpretation was regarded as not consistent with 'objective application of the law' and the impermissibility of general restriction of human rights that 'may not put in jeopardy the right itself'. Thus, the danger was seen in the potential for 'eroding protections for human rights guaranteed under international law' [McKune S., 2015].

However, is it really true to consider the draft Code simply as 'a food-for-thought document' [Grigsby A., 2015]? Besides a very modest impact of the Code at the universal level and till now rather futile attempts of Russia and China to place it as a possible source for new norm-creating[69], some

[65] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013). A/68/98. Para 18, Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement (accessed: 12.02.2022); GGE Report 2015, para 12.

[66] Available at: https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf; https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (accessed: 12.02.2022)

[67] UN General Assembly Resolution. 5 December 2018. A/RES/73/27.

[68] The Congress of United States of America. Resolution.26 March 2012. Available at: https://www.congress.gov/112/bills/hconres114/BILLS-112hconres114ih.pdf (accessed: 16.01.2022)

[69] Available at: https://dig.watch/sessions/norms-rules-and-principles (accessed: 12.02.2022)

of the key ideas of this draft were reflected in a number of both multilateral and bilateral treaties initiated by Russia and concluded with the states-members of the SCO and other states. Indeed, the concepts and threats identified by Russia, including 'use of information to undermine the political, economic and social system of other States', 'domination or control in the information area', and 'unauthorized transboundary influence through information' are clearly integrated within the SCO Agreement on Cooperation in the Field of International Information Security[70].

Chinese officials and scholars demonstrated continued support of the draft Code. On a number of occasions, China's Foreign Ministry's spokespersons characterized the Code of Conduct as the means of 'maintain[ing] peace and stability of the cyber space,' and declared that China was 'hoping to build a peaceful, secure, open and cooperative cyber space'.[71] Despite lacking recognition within the UN framework, Russia seems to retain its approach. Andrey Krutskikh, special representative of the President of the Russian Federation for international cooperation on information security, argued that 'the peace-oriented concept suggested by Russia has come in conflict with the position of several countries that seek to impose on the whole world their own game rules in the information space, which would only serve their own interests'.[72] Additionally, he stated existing approach 'puts in jeopardy the security interests of other countries and is fundamentally in contradiction with the objective of ensuring peace in the information space'[73].

Conclusion

In general, the impact of the choice of a standard-setting track examined in relation to the normativity of International law is ambivalent. On

[70] Available at: https://citizenlab.ca/2015/09/international-code-of-conduct/ (accessed: 12.02.2022)

[71] Available at: https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1164254.shtml; http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1241296.shtml; https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1242257.shtml (accessed: 12.02.2022)

[72] Available at: https://coe.mid.ru/en_GB/sotrudnicestvo-v-sfere-pravoporadka/-/asset_publisher/jYpWpmrO5Zpk/content/otvet-specpredstavitela-prezidenta-rossijskoj-federacii-po-voprosam-mezdunarodnogo-sotrudnicestva-v-oblasti-informacionnoj-bezopasnosti-a-v-krutskih-n?inheritRedirect=false&redirect=https%3A%2F%2Fcoe.mid.ru%3A443%2Fen_GB%2Fsotrudnicestvo-v-sfere-pravoporadka%3Fp_p_id%3D101_INSTANCE_jYpWpmrO5Zpk%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-1%26p_p_col_count%3D1 (accessed: 12.02.2022)

[73] Ibid.

the one hand, in the widely used ontological matrix of 'whether and how' International law applies to 'cyberspace', this track both strengthens the affirmative answer to the 'whether' question and helps to shape the contours of 'how', and, thus, clarifies the application of general and not cyber-specific legally binding norms of International law. Furthermore, the standard-setting can be a stage of the steady crystallization of the new international customary law or can serve as a platform for elaboration of a new international instrument, thus, paving the way for binding rules.

However, on the other hand, a positive effect of this track for the normativity of International law may be illusory and far from being neutral. Such scenarios can be enabled by both different combinations of the relationship of the content of such standards to the *lex lata* provisions of International law and the ways by which states will treat such non-binding norms. Should the endeavours of states be confined to standards not only in a short, but also in a middle and long term perspective, and binding rules will not be developed in the inter-state sphere where they are needed, it will mean that States are, thereby, championing a 'normative gap scenario'. A normative gap can also arise not because of the states' reluctance to make the standards formally binding, but stem from the content of these standards, if they will not bring any 'added value' to the existing legal framework. This will have an adverse impact on the International law as a legal regime, regardless of whether states would undertake any actions to codify such norms or not. Should the states follow the standard-setting track and adhere to the non-binding norms, provided that they are relaxing existing legal obligations of states, this 'deviation scenario' will also erode the normativity of International law.

References

1. Akande D., Coco A., Dias T. (2022) Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies. *International Law Studies*, no. 4, pp. 4–36.

2. Carr J. (2011) Four Problems with China and Russia's International Code of Conduct for Information Security. Available at: http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html.

3. D'Aspremont J. (2011) *Formalism and the Sources of International Law. A Theory of the Ascertainment of Legal Rules.* Oxford: University Press, 266 p.

4. D'Aspremont J. (2016) Cyber Operations and International Law: An Interventionist Legal Thought. *Journal of Conflict and Security Law,* no. 3, pp. 575–593.

5. Delerue F. (2020) *Cyber Operations and International Law.* Oxford: University Press, 549 p.

6. Dias T., Coco A. (2022) *Cyber Due Diligence in International Law.* Oxford: Institute for Ethics, Law and Armed Conflict, 256 p.

7. Doerr O., Schmalenbach K. (eds.) (2018) Vienna Convention on the Law of Treaties: A Commentary. Berlin: Springer, 1535 p.

8. Grigsby A. (2015) Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era. Available at: https://www.defenseone.com/voices/alex-grigsby/10825

9. Hollis D. (2020) Improving Transparency. International Law and State Cyber Operations. Fourth report to the Organization of American States. OEA/Ser.Q. CJI/doc. 603/20. Available at: http://www.oas.org/en/sla/iajc/current_agenda_Cyber-security.asp

10. Koh H.H. (2012) International Law in Cyberspace. *Harvard International Law Journal Online,* no. 54, pp. 1–12.

11. McKune S. (2015) An Analysis of the International Code of Conduct for Information Security. Available at: https://citizenlab.ca/2015/09/international-code-of-conduct

12. Mueller M. (2011) Russia & China Propose UN General Assembly Resolution on "Information Security". Available at: https://www.internetgovernance.org/2011/09/20/russia-china-propose-un-general-assembly-resolution-on-information-security/.

13. Schmitt M.T. (ed.) (2017) Tallinn Manual on the International Law Applicable to Cyber Operations. Cambridge: University Press, 598 p.

14. Schondorf R. (2020) Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. Available at: https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/

15. Segal A. (2012) China, International Law, and Cyberspace. Available at: https://thediplomat.com/2012/10/china-international-law-and-cyberspace

16. Shackelford S., Russell S., Kuehn A. (2016) Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors. *Chicago Journal of International Law,* no. 17, pp. 1–50.

17. Yeung K. (2017) 'Hypernudge': Big Data as a Mode of Regulation by Design. Information, *Communication & Society*, no. 1, pp. 118–136.

18. Zinovieva E. (2019) International cooperation in the field of information security: subjects and trends. Available at: https://mgimo.ru/upload/diss/2019/zinovieva-diss.pdf (in Russ.)

Information about the author

V.N. Rusinova — Professor, Doctor of Sciences (Law).

The article was submitted 15.12.2021; was approved after reviewing 19.01.2022; was accepted to publication 07.02.2022.