Russian Journal of World Politics and Law of Nations. 2022. 1(4). P. 32–46
DOI 10.24833/RJWPLN-2022-4-32-46 Research Article

Qualification of the Harmful Use of Information and Communications Technologies Under International Law: In Search of a Consensus[1]

Vera N. Rusinova

National Research University Higher School of Economics

Abstract. States face the question of how International Law norms should be applied to the harmful use of information and communications technologies (hereinafter ICT) in many different collective formats. Against this background, the intensive disclosure by states of their positions is a brand-new trend. As a result, managerialism is slowly giving way to consensualism. However, do these collective and individual efforts help to clarify the key problems connected with the qualification of these harmful practices? Based on the analysis of the reports of the UN Group of Governmental Experts and the Open-Ended Working Group, as well as the official positions articulated by states, this article seeks to reveal the extent to which states have managed to achieve a consensus on the qualification of harmful cyber activities under International Law, and on which issues. This question is crucial for identifying the subsequent practice in the application of international treaties, which establishes the agreement of the parties regarding their interpretation, as well as the practice and opinio juris as elements of international customs.

The research confirmed that the principle of non-intervention in domestic affairs, while its full applicability in the cyber context is not questioned by states, has very limited significance for the qualification of the harmful use of ICTs, which brings to the forefront the principle of sovereignty. However, the official positions of states, based on a denial or, vice versa, an affirmation of this principle as a separate rule, postulate the impossibility of applying the principle of sovereignty without the concretization of its content in the cyber context. The fact that there is a multitude of approaches does not foreshadow the possibility of reaching a consensus on this issue in the near future. With respect to the jus ad bellum and jus in bello norms, the readiness of the majority of states to qualify the cases of harmful use of ICTs as a "use of force" or even an "armed attack," and to overstretch the scope of the International Humanitarian Law notions of an "attack" or "military operation," is described as being indicative of the abuse of the "military paradigm" to assess these activities. The approaches of some states go so far beyond the normative scope of these notions that their assertion loses legal significance and seems to have rather a political character by primarily fulfilling the deterrent function.

[1] English translation from the Russian text: Rusinova V. N. 2022 Mezhdunarodno-pravovaia kvalifikatsiia vredonosnogo ispol'zovaniia informatsionno-kommunikatsionnykh tekhnologii: v poiskakh konsensusa. *Moskovskii Zhurnal Mezhdunarodnogo Prava [Moscow Journal of International Law].* No. 1. P. 38–51. https://doi. org/10.24833/0869-0049-2022-1-38-51.

The article concludes by diagnosing that a consensus between states on the application of International Law to harmful ICT practices has been reached at a very high level of abstraction and hardly transcends the limits of the general acknowledgment of the applicability of International Law in the cybersphere. This fact enshrines indeterminacy as the main feature of the qualification of harmful use of ICTs under International Law and renders almost every stance on nuances of the application of International Law to these acts to be ad hoc ones.

Keywords: cyberoperations, information and communications technologies, international information security, use of force, armed conflict, International Humanitarian Law, standards.

Countries are working feverishly to define and specify the norms of international law regarding the use of information and communications technologies (ICT) in various formats (Romashkina 2020). At the United Nations, two expert panels worked in parallel on the operationalization and updating of the "norms of responsible State behaviour," as well as on the development of an institutional dialogue and confidence-building measures in 2019–2021: the Sixth United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,[2] and the first Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.[3] The second working group has since started its work.[4] States take initiatives to adopt new standards,[5] develop new international treaties or become signatories of existing agreements on cooperating in combating ICT crime,[6] and enter into numerous bilateral agreements on the exchange of information and capacity

[2] Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. *UN: Note by the Secretary-General.* July 14, 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030R-1.pdf (accessed November 8, 2021).

[3] Final Substantive Report. *UN: Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.* March 10, 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed November 8, 2021).

[4] Developments in the Field of Information and Telecommunications in the Context of International Security. *UN: Resolution Adopted by the General Assembly.* December 31, 2020. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement (accessed November 8, 2021).

[5] International Code of Conduct for Information Security. Annex to the Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General. *UN*. September 12, 2011. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement (accessed November 8, 2021); International Code of Conduct for Information Security. 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. January 9, 2015. URL: https://daccess-ods.un.org/tmp/9398264.88494873.html (accessed November 8, 2021).

[6] Convention on Cybercrime. *Council of Europe.* November 23, 2001. URL: https://rm.coe.int/1680081561 (accessed November 8, 2021); Arab Convention on Combating Information Technology Offences. December 21, 2010. URL: https://unidir.org/cpp/en/multilateral-frameworks (accessed November 8, 2021).

building.[7] On May 10–12, 2021, a meeting of the Special Committee established by the UN General Assembly to develop a comprehensive international convention on combating the use of ICT for criminal purposes was held.[8]

In terms of their content, all these collective initiatives have a strong normative focus: they aim to clarify the interpretation of existing, or propose new, international laws to regulate activities related to the use of ICT. Recent years have been marked by the active disclosure by states themselves of their position on the main issues of this agenda. At the national level, Australia,[9] Great Britain,[10] Israel,[11] the Netherlands,[12] the United States (Koh 2012: 1–12), Finland,[13] France,[14] and Germany,[15] have clarified their positions in strategies, concepts and various official statements. As part of the work of the Group of Governmental Experts in 2021 to compile a compendium, some 15 states submitted their opinions on the application of international law to the use of ICT.[16] Nine responses came from a survey conducted by the Organization of American States (Hollis 2020: 5). The resulting meetings and preparatory work on the final report of the first Open-Ended Working Group proved to be a clear breakthrough: it was this format that allowed most countries to voice their positions on the issue.[17]

---

[7] According to an analysis conducted by the Center for International and Security Studies (University of Maryland), a total of 196 such agreements had been concluded by 116 states as of 2017 (Hitchens, Goren 2017).

[8] Countering the Use of Information and Communications Technologies for Criminal Purposes. *UN: Resolution of the General Assembly.* May 26, 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/54/PDF/N2113354.pdf?OpenElement (accessed November 8, 2021).

[9] Australia's International Cyber Engagement Strategy. Annex A: Australia's Position on the Application of International Law to State Conduct in Cyberspace. *Department of Foreign Affairs and Trade.* 2019. URL: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF (accessed November 8, 2021); Australia's International Cyber Engagement Strategy. Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace. *Department of Foreign Affairs and Trade*. 2017. URL: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf (accessed November 8, 2021).

[10] Cyber and International Law in the 21st Century. *UK Attorney General's Office.* May 23, 2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (accessed November 8, 2021).

[11] Schondorf R. Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *EJIL TALK!* 2020. URL: https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerningthe-application-of-international-law-to-cyber-operations/ (accessed November 8, 2021).

[12] Letter to the Parliament on the International Legal Order in Cyberspace. *Ministry of Foreign Affairs (The Netherlands).* July 5, 2019. URL: 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 November 8, 2021). Hereinafter, "Ministry of Foreign Affairs (the Netherlands)".

[13] International Law and Cyberspace. *Finland's National Positions.* 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyber-and-international-law-oct-2020.pdf (accessed November 8, 2021)

[14] International Law Applied to Operations in Cyberspace. *Ministère des Armées (France).* 2019. URL: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf (accessed November 8, 2021). Hereinafter, "Ministère des Armées (France)".

[15] Krieg im „Cyber-Raum" – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung. *Deutscher Bundestag.* December 10, 2015. URL: https://dserver.bundestag.de/btd/18/069/1806989.pdf (accessed November 8, 2021). S. 4–5, 7. (In German).

[16] 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. *UN*. 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-RU.pdf (accessed November 8, 2021). Hereinafter the "2021 Compendium".

[17] Open-Ended Working Group. *UN*. URL: https://www.un.org/disarmament/open-ended-working-group/ (accessed November 8, 2021).

However, can we draw the conclusion that all these efforts actually led to the clarification of at least the key issues related to the international legal qualification of the harmful use of ICT? The purpose of this paper is, with due account of the reports of the UN Group of Governmental Experts and the Open-Ended Working Group, as well as the official positions of individual states, to shed light on the extent to which, and on what issues, states have managed to reach a consensus on the application of the basic norms of international law with regard to what qualifies as the harmful use of ICT, as this is key to identifying both the subsequent practice of executing international treaties, which establishes the agreement of the participants regarding their interpretation,[18] and their implementation and opinio juris, as elements of new international customs.[19]

The Positions of States on Extending the Basic Rules of International Law to Cases of the Harmful Use of ICT

Let us take a look at general legal norms – those that were not created specifically to regulate the "cybersphere." In this case, the harmful use of ICT, in addition to the criminal legislation of individual states, may violate the principles of respect for sovereignty and non-interference in the affairs of other states, the ban on the use of and threats of the use of force, and, in the event of an armed conflict, the rules of international law. Hypothetically, such actions may also violate international human rights law. This is highly unlikely, however, given the limits on the extraterritorial application of the relevant international treaties, as well as the fact that many of these operations would be classed as "espionage," which is not prohibited by international law. The obligation to carry out due diligence, which requires states to ensure that, as the 2017 Tallinn Manual notes, their territories are not used as a base for state or non-state cyber operations against another state that would have serious consequences (Schmitt 2017: 30–50), is, to the extent that it goes beyond the general obligation of states "not to allow knowingly its territory to be used for acts contrary to the rights of other States," as established by the International Court of Justice in the *Corfu Channel Case*,[20] still in its infancy (Chircop 2018: 667–668), and, despite the position of some states,[21] is considered *lex ferenda* (Shackelford, Russell, Kuehn 2016: 22–23; Delerue 2020: 353–376; Jensen, Watts 2017: 1573–1574).[22] Based on these considerations, the following analy-

[18] Article 31, Clause 3 (b) of the Vienna Convention on the Law of Treaties dated May 23, 1969. *Vedomosti of the Supreme Soviet of the Soviet Union,* 37. September 10, 1986. P. 772.

[19] Article 38 of the Statute of the International Court of Justice dated June 26, 1945. In Y.M. Kolosov and E.S. Krivchikova, eds., *Current International Law*. Vol. 1. Moscow: 1999. P. 797.

[20] International Court of Justice: Corfu Channel Case (UK v. Albania). Judgment of 9 April 1949. *ICJ. Reports*. 1949, 4.

[21] Ministry of Foreign Affairs (the Netherlands), 4–5; Ministère des Armées (France), 9–10.

[22] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *UN: Note by the Secretary-General.* June 22, 2015. URL: https://digitallibrary.un.org/record/799853/files/A_70_174-RU.pdf (accessed November 8, 2021), §13(c). Hereinafter the "2015 UN GGE Report." See also: U.S. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. 2011. URL: http://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed November 8, 2021), § 10.

sis will be limited to the three main blocks of the basic norms of international law: 1) the principles of respect for sovereignty and non-interference in the internal affairs of other states; 2) international security law; and 3) international humanitarian law.

The Principles of Respect for Sovereignty and Non-Interference in the Internal Affairs of Other States

The attitude of states towards the application of the two principles of international law in relation to cases of the harmful use of ICT – the principle of respect for sovereignty and non-interference in the internal affairs of other states – very clearly reflects the dichotomy between those types of interference that states do not want to be perpetrated against themselves, and those that they would like to be able to use against other states (Rusinova 2018: 41-49). This is manifested in two cases.

First, states have set a rather high bar when it comes to the application of the principle of non-intervention in the internal affairs of other states that does not involve ICT, and one that is very difficult to achieve. The quintessence of this approach is the two-tier test formulated by the International Court of Justice in the case of Nicaragua v. United States of America in 1986.[23] According to the judgement, the principle of non-interference is considered violated if, first, it bears "on matters in which each State is permitted, by the principle of State sovereignty. to decide freely,"[24] (or *domaine reserve*), and, second, "methods of coercion in regard to such choices, which must remain free ones" are used.[25] This is comparable to casting a net with very wide meshes. The same approach applies to cases of ICT use. This principle of non-intervention, which stands apart in terms of its limited scope, thus becomes practically useless when it comes to the use of ICT. This follows from the fact that there is no element coercion in most cases of the malicious use of ICT: attacks on computer networks that are intended to cause damage, obtain a ransom, exact revenge, or steal information do not satisfy this criterion. At the same time, some states attempt to interpret the *domaine reserve* criterion as related not only to the state's exercising of its power, but also as a "shield for entire policy areas."[26] This is primarily due to the attempt of states to protect themselves from interference in elections. The extent to which this approach can be taken is observed in the example of Norway, which declared that unlawful interference in internal affairs is intended to "unduly influence public opinion."[27] At the same time, such attempts are mostly isolated: even when states spot interference in elections, most of them nevertheless refer to the need to apply the general two-tier test to this type of interference.[28]

---

[23] International Court of Justice: Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Judgment of 27 June 1986. *ICJ. Reports.* 1986, 14. Para. 240. Hereinafter the "Case Concerning Military and Paramilitary Activities in and against Nicaragua."

[24] Ibid. Para. 205

[25] Ibid.

[26] Ziegler K.S. Domaine Réservé. In *The Max Planck Encyclopedia of Public International Law,* ed. R. Wolfrum. Vol. III. Oxford: Oxford University Press. 2012. P. 213.

[27] 2021 Compendium (Norway), 69.

[28] 2021 Compendium (Brazil), 19.

In general, the principle of non-interference plays a minor role when it comes to assessing the legality of the harmful use of ICT. And, at present, election meddling is perhaps the only example that illustrates attempts to modify the scope of this principle. It is from here that the principle of respect for sovereignty, arising from the principle of the sovereign equality of states, comes to the fore. While this principle is closely related to the principle of non-intervention in the internal affairs of other states, it follows from the decision of the International Court of Justice in the case of Nicaragua v. United States of America that their content is not identical, and the principle of respect for territorial sovereignty can be violated by actions that do not qualify as a violation of the principle of non-intervention. Overflights of American aircraft over Nicaraguan territory were recognized as just such a violation.[29] However, a common test for verifying compliance with this principle, in contrast to the principle of non-intervention, has not been developed either in state practice or in doctrine.

We should note here that, when compiling the Tallinn Manual, experts were seriously divided in their opinions regarding the lower threshold for actions to be considered a violation of the principle of respect for sovereignty and the range of infrastructure facilities that fall under its protection (Schmitt 2017: 20–27). And the positions of states were even further apart. The United States and the United Kingdom have stated that the principle of respect for sovereignty is a "general principle," "a fundamental concept in international law," but not a rule of law.[30] That is, this principle is not a separate rule that can be violated if the use of ICT cannot be qualified as a violation of the principle of non-intervention in the internal affairs of other states.

In response, several states argued the normative nature of the principle of respect for sovereignty. At the same time, the Netherlands, Finland and Switzerland referred to the approach reflected in the 2017 Tallinn Manual, which states that this principle would be violated if territorial integrity had been encroached upon or the performance of public functions had been usurped or interfered with,[31] and stressed to need to apply a lower threshold.[32] Some countries, for example Brazil, Norway and France, have

[29] Case Concerning Military and Paramilitary Activities in and against Nicaragua, paras. 251, 292.

[30] The Application of International Law to State Cyberattacks Sovereignty and Non-Intervention. *Chatham House Research Paper.* 2019. URL: www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf (accessed November 8, 2021); Cyber and International Law in the 21st Century. *UK Attorney General's Office.* May 23, 2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; 2021 Compendium (United Kingdom), 117, Para. 10.

[31] 2021 Compendium (the Netherlands), 56–57; 2021 Compendium (Switzerland), 87; Finland's National Positions, International Law and Cyberspace (2020), 2–3.

[32] Letter to the Parliament on the International Legal Order in Cyberspace. *Ministry of Foreign Affairs (the Netherlands).* July 5, 2019. URL: 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 November 8, 2021); Schmitt M. The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis. Just Security. 2019. URL: www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis (accessed November 8, 2021); International Law and Cyberspace. *Finland's National Positions.* 2020. URL: www.front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyberand-international-law-oct-2020.pdf (accessed November 8, 2021).

tried to adhere to the broadest possible approach to the content of this principle. As the French Ministry of Defence has pointed out, the country's sovereignty is violated by any cyberattack on, first, "information systems located on its territory," including "equipment and infrastructure located on national territory; connected objects [and their] logical components,", second, "content operated or processed via electronic communication networks which cover the national territory or from an IP address attributed to France," and, third, "domains belonging to national registers."[33] Norway put forward a similar position,[34] and Brazil's extremely broad approach can be judged by the fact that it named "interceptions of telecommunications" as an example of a violation of sovereignty.[35]

Legal positions based on the denial or, conversely, the recognition of the normative nature of the principle of respect for sovereignty are, despite their seeming incompatibility, not that far from each other, as both state that it is impossible to apply this principle without specifying its content in relation to the use of ICT. The only difference is that this conclusion is explicit in the first case, and implicit in the second, since the variety of approaches to the content of the principle of respect for sovereignty articulated by states that insist on the normativity of this principle ultimately indicates the absence of such a rule, which could apply to ICT. However, the multiplicity of the positions of states does not portend the possibility of reaching a consensus on this issue in the foreseeable future.

International Security Law

The application of jus ad bellum norms regarding the legality of the use of force in international relations is based on a two-pronged approach arising from the UN Charter, which draws a distinction between the concepts of the "use of force" (Article 2, Paragraph 4) and "armed attack" (Article 51).[36] The International Court of Justice notes that this approach is based on the application of different minimum thresholds, depending on the "scale and effects" of the use of force.[37] The readiness of most states to classify cases of the malicious use of ICT as a "use of force" or an "armed attack," even outside the framework of an armed attack, indicates an abuse of the "military paradigm" when it comes to assessing these actions. This conclusion in based on three premises: 1) the repeatedly used argument about the uncertainty of the minimum threshold for the concepts of the "use of force" and "armed attack"; 2) the use of the analogy with kinetic attacks; and 3) the use of long chains of causality (Corten 2012: 5–27).

[33] Ministère des Armées (France), 9–10.
[34] 2021 Compendium (Norway), 68.
[35] 2021 Compendium (Brazil), 18.
[36] Article 2, Paragraph 4, Arcile 51 of the UN Charter; Case Concerning Military and Paramilitary Activities in and against Nicaragua, § 191.
[37] Ibid., § 195.

The well-established interpretation of *jus ad bellum* does indeed proceed from the fact that the prohibition on the use of force may be violated, regardless of the type of weapon used,[38] and is based on a causal relationship between the use of force and the consequences. Accordingly, the destructive power of a weapon may not be kinetic; it could be chemical or bacteriological. And, because the consequences of its use are comparable to those of a kinetic weapon (causing death or injury, destroying facilities), the use of such weapons will fall under the concept of the "use of force" or an "armed attack" as set out in the UN Charter.[39] In the case of the use of ICT, however, the chain of consequences can be substantially longer than with the traditional use of weapons. On the one hand, it would be wrong to deny that some types of malicious computer programs can assume military forms, and it would be correct from a legal point of view to assess them in terms of *jus ad bellum*. On the other hand, applying this analogy to long chains of causation will inevitably take us beyond the line where the similarities between the use of ICT and kinetic attacks will directly contradict the consensus of states on the interpretation of the scope of the concept of the "use of force" as not extending to non-military forms of influence such as "economic coercion" (Simma 2002: 118).

At the same time, the positions articulated by the members of the Open-Ended Working Group in 2019–2020 only confirm the popularity of drawing an analogy between the use of ICT and kinetic attacks.[40] Only four countries expressed doubts and concerns in this regard. Brazil and India pointed to the ambiguity surrounding the minimum thresholds of what constitutes the "use of force" and an "armed attack," while Pakistan was concerned about the applicability of Article 51 of the UN Charter to "cyber operations." Russia was harshest of all in its criticism, stating that the concepts of "use of force" and "armed attack" can only be applied in the context of an armed conflict, and a cyberattack outside such a context does not fall under either definition.[41]

---

[38] International Court of Justice: Legality of the Threat or Use of Nuclear Weapons. Advisory Opinion of 8 July 1996. *ICJ. Reports*. 1996, 226, § 39.

[39] Ibid.

[40] Second Substantive Session. *Open-Ended Working Group (OEWG)*. 2020. URL: https://dig.watch/events/open-ended-working-group-oewg-second-substantive-session (accessed November 8, 2021); Australia's Cyber Engagement Strategy. Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace. *Department of Foreign Affairs and Trade*. 2019. URL: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF (accessed November 8, 2021); Australia's Cyber Engagement Strategy. Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace. *Department of Foreign Affairs and Trade*. 2017. URL: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf (accessed November 8, 2021); On the Application of International Law in Cyberspace. *Federal Government (Germany) Position Paper*. 2021. URL: www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf (accessed November 8, 2021), P. 5-6; Cyber and International Law in the 21st Century. *UK Attorney General's Office*. May 23, 2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (accessed November 8, 2021). See also (Koh 2012: 1–12).

[41] Second Substantive Session. *Open-Ended Working Group (OEWG)*. 2020. URL: https://dig.watch/events/open-ended-working-group-oewg-second-substantive-session (accessed November 8, 2021).

However, even if the correctness of the analogy and causality approach is not challenged, many of the known cases of malicious use of ICT would not be classified as "use of force" due to their low intensity (scale and effects) (Watts 2015: 249–250).[42] This is a serious limitation on the application of the "military paradigm," which may explain why a number of states, by formulating their positions at the national level, want to influence the formation of a common approach to determining where exactly the issue of the minimum thresholds of what constitutes the "use of force" and an "armed attack" will be located in the context of the use of ICT, and in particular to keep these thresholds as low as possible.

For example, France has established that even a "cyberoperation without physical effects may also be characterised as a use of force," and has drawn up what we should note is a non-exhaustive list of criteria that should be applied in such as assessment. These include: "the origin of the operation and the nature of the instigator (military or not), the extent of intrusion, the actual or intended effects of the operation or the nature of the intended target."[43] The Dutch Minister of Foreign Affairs also stated that, "it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force."[44] Finally, the United Kingdom's Cyber Primer, while recognizing the need for an operation to cause the same or comparable impact as a kinetic attack in order to fall under the concept of the "use of force" under Article 2, Paragraph 4 of the UN Charter, states in a footnote that prolonged attacks on the UK banking system that can cause serious financial damage to the state, leading to the deterioration in the economic security of the population may qualify as such.[45] Norway's position on determining the range of actions that can be classified as the "use of force" is among the broadest.[46] It would appear that in their understandings of the "use of force" and "armed attack," states deviate so far from the normative content of these concepts that advocating these approaches acquires limited legal potential and is rather of a political nature, performing the function of deterring potential threats.

International Humanitarian Law

While the Group of Governmental Experts confirmed back in 2015 that the scope of the UN Charter can be extended to the sphere of ICT, international humanitarian law has remained the last bastion of controversy in this area. Only four principles were noted in the 2015 report: humanity, necessity, proportionality and distinction.

---

[42] Significant Cyber Incidents Since 2006. *Center for Strategic and International Studies*. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/200626_Cyber_Events.pdf (accessed November 8, 2021).

[43] Ministère des Armées (France), 7.

[44] Ministry of Foreign Affairs (the Netherlands), 4.

[45] Cyber Primer. Annex 1A – International Law Aspects. 2nd ed. *UK Ministry of Defence*. 2016. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf (accessed November 8, 2021), P.12.

[46] 2021 Compendium (Norway), 70.

Meanwhile, the final reports in 2016 and 2017 were not adopted by the Group of Governmental Experts due, among other things, to these disagreements. The 2021 report finally acknowledged the applicability of "international humanitarian law," but, as the Sixth Panel clarified, only in situations of armed conflict.[47] This acknowledgement thus proved to be ambivalent: while the document does point to the norms of international humanitarian law instead of separate principles, the issue of whether an operation using ICT can qualify as an "armed conflict" was not resolved and will therefore continue to be open to various readings in the future.

In general, most states have confirmed the applicability of international humanitarian law (*jus in bello*) to ICT operations. The counter argument to this, put forward by states such as China, Cuba, Pakistan, Russia and Syria,[48] is that it would legitimize the militarization of "cyberspace." A superficial interpretation of this argument may lead one to the conclusion that this goes against the entire history of the development of *jus in bello* norms. However, this argument can also mean that the misuse of the "military paradigm" can be caused, on the one hand, by the lack of a clear dividing line between the "military use" of ICT, which may qualify as the "use of force" or an "armed attack" according to the *jus ad bello* concept, and, on the other hand, by the "non-military use" of ICT – an action in the field on computer information that can be criminalized under national law and which can be carried out, among other things, against the background of an armed conflict. Thus, the *jus in bello* concept will displace the "law enforcement paradigm": the application of international human rights law or domestic criminal law, which, in turn, may very well be based on international treaties on the criminalization of the harmful use of ICT.

What is more, we should not lose sight of the fact that the conceptual apparatus of international humanitarian law does not fit in a number of cases, nor does it allow for the norms governing activities in this industry to be used in relation to computer code. Thus, the large-scale confirmation of the applicability of international law in this area will either lead to disappointment, where the norms of international humanitar-

---

[47] Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. *UN: Note by the Secretary-General.* July 14, 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030R-1.pdf (accessed November 8, 2021), § 71(f).

[48] Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Just Security.* June 23, 2017. URL: https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf (accessed November 8, 2021); Response of the Special Representative of the Russian Federation for International Information Security A.V. Krutskikh to the Question of the TASS News Agency on the State of the International Dialogue in this Area. *Ministry of Foreign Affairs of the Russian Federation.* June 29, 2017. URL: http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288 (accessed November 8, 2021). On China's position, see: Korzak E. UN GGE on Cybersecurity: The End of an Era? *The Diplomat.* July 31, 2017. URL: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ (accessed November 8, 2021); First Substantive Session. *Open-Ended Working Group (OEWG).* 2019. URL: https://dig.watch/event/open-ended-working-group-oewg-first-substantive-session (accessed November 8, 2021); Second Substantive Session. *Open-Ended Working Group (OEWG).* 2020. URL: https://dig.watch/events/open-ended-working-group-oewg-second-substantive-session (accessed November 8, 2021).

ian law can only be applied to the extent of general principles and the categorization of individuals, and no further, or start to fuel the desire to stretch existing international legal concepts to cover the use of ICT. To be sure, there are at least three areas in which the application of international humanitarian law to the field of ICT may be extremely problematic.

First, if we do not stretch the concept of "attack" as laid out in international humanitarian law to the harmful use of ICT, then the question of the insufficiency of the norms in this industry will inevitably arise. This is a result of the succinctness of the provisions of *jus in bello* with regard to "military operations," and even to an international armed conflict (such provisions do not exist for conflicts that are not international in nature). However, most cases of the malicious use of ICT would not be classified as "attacks," and at best can be qualified as "military operations." With regard to Article 51, Paragraph 1 and Article 57, Paragraph 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1), the obligations of the parties to a conflict are too broadly and are limited to imposing the obligation to provide "general protection" to the civilian population "against dangers arising from military operations," and that "constant care shall be taken to spare the civilian population, civilians and civilian objects."

The limited applicability of the category of "attack" under international humanitarian law to operations using ICT is reflected in the position of France. As we know, the Ministère des Armées adopted an extremely broad approach to what can be considered the "use of force" according to *jus ad bellum*, where operations that do not cause physical damage are considered as such. However, the same was not done with regard to what constitutes an "attack," and the Ministère was thus forced to admit that "Most cyberoperations, including offensive cyber warfare operations carried out by France in an armed conflict situation, remain below the attack threshold," and, as such, they "remain nonetheless governed by the general principles of IHL."[49]

Second, a problem arises when countries try to circumvent the *jus in bello* limitations of the concept of an "attack" by stretching its scope to include as many types of malicious use of ICT as possible. For example, the American legal adviser Brian Egan noted that while "Not all cyber operations […] rise to the level of an "attack" as a legal matter under the law of armed conflict," it is nevertheless possible to qualify such operations as "attacks" considering, "among other things, whether a cyber activity results in kinetic or non-kinetic effects, and the nature and scope of those effects, as well as the nature of the connection, if any, between the cyber activity and the particular armed conflict in question."[50] The use of such an approach may lead to the objective inap-

[49] Ministère des Armées, 13.

[50] Egan B.J. Remarks on International Law and Stability in Cyberspace. Speech at Berkeley Law School. November 10, 2016. URL: 2009-2017.state.gov/s/l/releases/remarks/264303.htm (accessed November 8, 2021).

plicability of the rules of international humanitarian law on "attacks" to cases of the harmful use of ICT, because these rules were conceived and formulated in such a way as to regulate kinetic operations.

The third problem related to the applicability of international humanitarian law to the harmful use of ICT stems from the fact that the perpetrators of a given action may be associated, to varying degrees, with a state or non-state party to an armed conflict. This, together with the special nature of ICT activity itself, could cause the key category for international humanitarian law in the various readings presented in the legal literature (Melzer 2009: 46–64) and in judicial decisions[51] – namely "direct participation in hostilities" – to be insufficiently broad in its scope. Both the requirement for the perpetrator to have close ties with a party to the conflict in order to classify them as a combatant or a member of an organized armed force or group, and the requirement for kinetic or kinetic-like damage, a direct causal link, and a connection to the hostilities may lead to this result.

The Unclear Prospects for Law-Making: Standards instead of Norms

Despite the significant number of challenges that applying the general rules of international law *lex lata* to the malicious use of ICT brings, the role of law-making in this process is still quite small. States themselves, or at least the vast majority of them, prefer not to tie themselves down to any new obligations (Delerue 2019: 315–316). And countries have gone on record with their reasons for this: the existing "strategic framework" for the regulation of "cyberspace" is sufficient (the European Union, Portugal); creating new legally binding norms may threaten to blur existing norms or generate uncertainty regarding their status (Bulgaria, Italy); current state practice is insufficient (Israel); there is a lack of consensus among states (the United Kingdom); and the international rule-making process lags seriously behind the speed of technological development (the United States, Singapore, the United Kingdom, Australia). Only a small number of countries have indicated a preference for the law-making track (Algeria, Nigeria, Russia, Syria, and the countries of the Caribbean Community), while some of them have additionally noted that they are considering the need to create new rules in the medium or long term only (South Africa, Chile, Brazil). The development of new international norms is still limited to the level of cooperation between states in combating IT-related crime.[52]

---

[51] Supreme Court of Israel: The Public Committee against Torture in Israel v. the Government of Israel et al. Judgment of 13 December 2006. URL: http://elyon1.court.gov.il/Files_ENG/02/690/007/a34/02007690.a34.htm (accessed November 8, 2021), § 39.

[52] See: Interview with the Director of the Department of International Information Security of the Ministry of Foreign Affairs of the Russian Federation A.V. Krutskikh "The Global Cyber Agenda" with the *International Affairs* Newspaper. *Ministry of Foreign Affairs of the Russian Federation.* June 7, 2021, URL: https://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/4778945 (accessed November 8, 2021).

The consensus-based process of formulating "standards" has taken centre stage. However, the content of the standards that have been approved by the UN General Assembly – both in their original form (the 11 "voluntary, non-binding norms for responsible state behaviour")[53] and in their expanded version (the 14 "rules of conduct")[54] – have not brought any "added value" to assessing the legality of the malicious use of ICT compared to existing norms.[55] Each standard that is formulated as being applicable to this assessment is necessarily limited to referring to the rules of international law that are currently in force. Moreover, all "rules or principles of responsible behaviour" are subject to the general proviso that they "do not seek to limit or prohibit action that is otherwise consistent with international law."[56] The standard-setting approach can be important and justified as a policy tool to further validate the applicability of international law to ICT-related activities (Akande, Coco, de Souza Dias 2022: 34). However, the "norms of responsible behaviour" are legally tautological in their content, as they do not add anything new to the assessment of the legality of the harmful use of ICT.

Conclusion

The articulation by states of their positions on how exactly the norms of international law should be applied to malicious ICT operations indicates that managerialism is gradually retreating, giving way to consensualism. However, as our analysis of the approaches taken by states demonstrates, a consensus has developed at a very high level of abstraction and is unlikely to go beyond recognizing that the scope of the general rules of international law should be extended to ICT. This fixes uncertainty as a key characteristic of the international legal assessment of relevant cases and makes almost any judgement about the nuances of applying international law in the "cybersphere" an *ad hoc* conclusion that is voluntaristic and challengeable. Perhaps this circumstance explains the fact that states, when responding to cases of the malicious use of ICT, prefer to choose political rather than logical rhetoric. And if they do turn to the law, they use national (in the case the United States) or supranational (in the case of the European Union) standards via coercive measures (so-called "sanctions"[57]). This

[53] 2015 UN GGE Report. Para. 13.

[54] Developments in the Field of Information and Telecommunications in the Context of International Security. UN. December 5, 2018. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement (accessed November 8, 2021).

[55] It is noteworthy that the only country to speak in favour of transforming the rules of responsible behaviour developed by the GGE into legally binding norms during the meetings of the Open-Ended Working Group was Egypt. The Philippines lamented the non-binding nature of these recommendations and the limited scope for their implementation.

[56] 2015 UN GGE Report. Para. 10.

[57] This term is used in international law to mean coercive measures taken by an international organization in accordance with its charter. Accordingly, the use of this term in national law is much broader and covers all coercive measures that are designed to exert pressure on a foreign state, and their legality is not made dependent on the commission of an internationally wrongful act by that state.

approach (Roscini 2015: 248–254) allows states to bypass most of the limitations and complexities associated with the application of both the basic rules of international law, and the secondary norms requiring compliance with internationally recognized standards of proof and the disclosure of evidence.

About the Author:

Vera N. Rusinova – Doctor of Sciences (Law), Professor, Head of the School of International Law, Faculty of Law, National Research University Higher School of Economics. 20, ul. Myasnitskaya, Moscow, Russian Federation, 101000. ORCID: 0000-0002-5838-0283. E-mail: vrusinova@hse.ru.

Conflict of interests:
The author declares the absence of any conflict of interest.

References:

Akande D., Coco A., de Souza Dias T. 2022. Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies. *International Law Studies.* Vol. 99. P. 4-36.

Chircop L. 2018. A Due Diligence Standard of Attribution in Cyberspace. *International and Comparative Law Quarterly.* 67(3): 643-668. DOI: 10.1017/ S0020589318000015.

Corten O. 2012. *The Law against War: The Prohibition on the Use of Force in Contemporary International Law.* Oxford; Portland: Hart Publishing. 569 p.

Delerue F. 2019. Reinterpretation or Contestation of International Law in Cyberspace? *Israel Law Review.* 52(3): 295-326. DOI:10.1017/S0021223719000104.

Delerue F. 2020. *Cyber Operations and International Law.* Cambridge: Cambridge University Press. 513 p. DOI: https://doi.org/10.1017/9781108780605.

Hitchens Th., Goren N. 2017. *International Cybersecurity Information Sharing Agreements.* 141 p. URL: https:// cissm.umd.edu/sites/default/files/2019-07/Cyber%20information%20sharing%20agreement%20report%20-%20102017%20%20FINAL.pdf (accessed 01.11.2021).

Hollis D. 2020. *Improving Transparency. International Law and State Cyber Operations. Fourth report to the Organization of American States.* 22 p. URL: https://ceipfiles. s3.amazonaws.com/pdf/ CyberNorms/LawStatements/ Improving+Transparency+International+Law+and+St ate+Cyber+Operations_+Fourth+Report.pdf (accessed 01.11.2021).

Melzer N. (ed). 2009. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law.* Geneva: International Committee of the Red Cross. 89 p. URL: www.icrc.org/en/doc/assets/ files/other/icrc-002-0990.pdf (accessed 01.11.2021).

Jensen E.T., Watts S. 2017. A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? *Texas Law Review.* Vol. 95. P. 1555-1577.

Koh H.H. 2012. International Law in Cyberspace. *Harvard International Law Journal Online.* Vol. 54. P. 1-12. URL: https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf (accessed01.11.2021).

Romashkina N. P. 2020. Problema mezhdunarodnoi informat- sionnoi bezopasnosti v OON [Problem of International Information Security in the UN]. *Mirovaya ekonomika i mezhdunarodnye otnosheniya.* No.64. P. 25-32. DOI: 10.20542/0131-2227-2020-64-12-25-32. (In Russian).

Roscini M. 2015. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal.* 50(2): 233-273.

Rusinova V. N. 2018. Mezhdunarodno-pravovoi printsip nevmeshatel'stva i kiberoperatsii: neopravdannye ozhidaniya? [The international legal principle of noninterference and cyber-operations: unjustified expectations?]. *Mezhdunarodnoe pravosudie.* No. 1. P. 38-52. DOI: 10.21128/2226-2059-2018-1-38-52. (In Russian).

Shackelford S.J., 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.* Vol. 17. P. 1-51.

Schmitt M. N. (ed). 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Ed. by Cambridge: Cambridge University Press. 598 p.

Simma B. (ed). 2002. *The Charter of the United Nations. A Commentary.* 2nd ed. Oxford: Oxford University Press. 895 p.

Watts S. 2015. Low-Intensity Cyber Operations and the Principle of Non-Intervention. In: Ohlin J.D., Govern K., Finkelstein C. (eds). *Cyber War: Law and Ethics for Virtual Conflicts.* Oxford: Oxford University Press. P. 249-270. DOI: 10.1093/acprof:oso/9780198717492.003.0012