DOI: https://doi.org/10.24833/0869-0049-2022-1-38-51

Исследовательская статья
Поступила в редакцию: 10.11.2021
Принята к публикации: 01.03.2022

Вера Николаевна РУСИНОВА
Национальный исследовательский университет «Высшая школа экономики»
Мясницкая ул., д.20, Москва, 101000, Российская Федерация
vrusinova@hse.ru
ORCID: 0000-0002-5838-0283

МЕЖДУНАРОДНО-ПРАВОВАЯ КВАЛИФИКАЦИЯ ВРЕДОНОСНОГО ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: В ПОИСКАХ КОНСЕНСУСА

ВВЕДЕНИЕ. *Интенсивная работа по конкретизации норм международного права в отношении использования информационно-коммуникационных технологий (далее – ИКТ) ведётся государствами в различных коллегиальных форматах. При этом отличительной особенностью последних лет стало активное раскрытие самими государствами своей позиции по основным дискуссионным вопросам этой повестки. Так менеджериализм стал постепенно уступать место консенсуализму, но возникает вопрос: привели ли коллективные и индивидуальные усилия государств к прояснению, по меньшей мере, ключевых проблем, связанных с международно-правовой квалификацией вредоносного использования ИКТ?*

МАТЕРИАЛЫ И МЕТОДЫ. *Данная статья призвана, учитывая как доклады Группы правительственных экспертов ООН и Рабочей группы открытого состава, так и официальные позиции отдельных государств, пролить свет на то, в какой степени и по каким вопросам применения первичных норм международного права для квалификации вредоносного использования ИКТ государствам удалось достичь консенсуса, поскольку именно он важен при выявлении как последующей практики применения международных договоров, которая устанавливает соглашение участников относительно их толкования, так и практики и opinio juris, как элементов новых международных обычаев.*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *На основании проведённого анализа было выявлено, что принцип невмешательства во внутренние дела, который признаётся государствами применимым в «киберсфере» в том же объёме, что и в других, имеет очень ограниченное значение для квалификации вредоносного использования ИКТ. Отсюда, на первый план выходит принцип уважения суверенитета. Однако правовые позиции, основанные на отрицании или, наоборот, признании нормативности принципа уважения суверенитета, постулируют невозможность применить данный принцип без конкретизации его содержания в отношении использования ИКТ. Полифоничность позиций государств не предвещает возможности достичь консенсуса по этому вопросу в обозримом будущем. Что касается норм jus ad bellum и jus in bello, то готовность большинства государств квалифицировать случаи вредоносного использования ИКТ как «применение силы» или даже «вооружённое нападе-*

ние» даже вне рамок вооружённого конфликта, а также перерастягивать объём таких понятий международного гуманитарного права как «нападение» или «военная операция», свидетельствует о злоупотреблении «военной парадигмой» при оценке таких деяний. Ряд государств настолько далеко отходят от нормативного содержания этих понятий, что отстаивание данных подходов приобретает ограниченный юридический потенциал, и, скорее, носит политический характер, выполняя функцию сдерживания потенциальных угроз.

ОБСУЖДЕНИЕ И ВЫВОДЫ. *В статье обосновывается общий вывод о том, что консенсус о применении международного права к случаям вредоносного использования ИКТ сложился на очень высоком уровне абстракции и вряд ли выходит за пределы признания распространения сферы действия общих норм международного права на ИКТ. Это закрепляет неопределённость в качестве ключевой характеристики международно-правовой оценки соответствующих случаев и делает практически любое суждение о нюансах применения норм международного права в «киберсфере» выводом ad hoc.*

КЛЮЧЕВЫЕ СЛОВА: *кибероперации, информационно-коммуникационные технологии, международная информационная безопасность, применение силы, вооружённый конфликт, международное гуманитарное право, стандарты*

ДЛЯ ЦИТИРОВАНИЯ: Русинова В. Н. 2022. Международно-правовая квалификация вредоносного использования информационно-коммуникационных технологий: в поисках консенсуса. – *Московский журнал международного права.* No.1. С. 38–51. DOI: https://doi.org/10.24833/0869-0049-2022-1-38-51

Автор заявляет об отсутствии конфликта интересов.

MASS INFORMATION AND INTERNATIONAL LAW

DOI: https://doi.org/10.24833/0869-0049-2022-1-38-51

Research article
Received 10 November 2021
Approved 1 March 2022

Vera N. RUSINOVA
National Research University "Higher School of Economics"
20, ul. Myasnitskaya, Moscow, Russian Federation, 101000
vrusinova@hse.ru
ORCID: 0000-0002-5838-0283

QUALIFICATION OF HARMFUL USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES UNDER INTERNATIONAL LAW: IN SEARCH OF A CONSENSUS

INTRODUCTION. *States are seized with the question of how International Law norms should be applicable with respect to harmful use of information and communications technologies (hereinafter – ICT) in many different collective formats. Against this background, an intensive disclosure of the states' positions is a brand new*

trend. So, managerialism is slowly giving way to consensualism, however, do these collective and individual efforts help to clarify, at least, the key problems connected with the qualification of these harmful practices?

MATERIALS AND METHODS. *Being 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 on which questions and in which volume states have managed to achieve a consensus on the qualification of harmful cyber activities under International Law. This question is crucial for the identification of 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.*

RESEARCH RESULTS. *The research confirmed that the principle of non-intervention into domestic affairs, albeit its full applicability in cyber context is not being questioned by the states, has a very limited significance for the qualification of the harmful use of ICTs, which brings to the forefront the principle of sovereignty. However, the states' official positions, based on a denial or, vise versa, an affirmation of this principle as a separate rule, postulate the impossibility to apply the principle of sovereignty without concretization of its content in the cyber context. The polyphony of the approaches does not foreshadow a possibility to reach consensus on this issue in the nearest 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. Approaches of some states go beyond the normative scope of these notions so far that their assertion loses legal significance and seems to have rather a political character by primarily fulfilling the deterrent function.*

DISCUSSION AND CONCLUSIONS. *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 the 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 an ad hoc one.*

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

FOR CITATION: Rusinova V. N. Qualification of Harmful Use of Information and Communications Technologies under International Law: In Search of a Consensus. – *Moscow Journal of International Law.* 2022. No. 1. P. 38–51. DOI: https://doi.org/10.24833/0869-0049-2022-1-38-51

The author declares the absence of conflict of interest.

1. Введение

Интенсивная работа по конкретизации норм международного права в отношении использования информационно-коммуникационных технологий (далее – ИКТ) ведётся государствами в различных форматах [Ромашкина 2020]. На уровне ООН над операционализацией и дополнением «норм ответственного поведения государств», а также развитием институционального диалога и мер по укреплению доверия в 2019-2021 гг. параллельно работали две коллегии экспертов: шестая Группа правительственных экспертов ООН[1] и первая Рабочая группа открытого состава[2]. На текущий момент к работе приступила вторая

[1] ООН: Записка Генерального секретаря «Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности. 14.07.2021. Доступ: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030R-1.pdf (дата обращения: 08.11.2021).

[2] UN: Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Final Substantive Report. March 10, 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed 08.11.2021).

группа[3]. Государства выступают с инициативами принятия новых стандартов[4], разрабатывают новые международные договоры или присоединяются к существующим соглашениям о сотрудничестве в области борьбы с правонарушениями в сфере ИКТ[5], заключают многочисленные двусторонние соглашения об обмене информацией и развитии потенциала[6]. 10 – 12 мая 2021 г. состоялось организационное собрание учреждённого Генеральной Ассамблеей ООН Специального комитета, который призван разработать всеобъемлющую международную конвенцию о противодействии использованию ИКТ в преступных целях[7].

С точки зрения содержания, все эти коллективные инициативы имеют ярко выраженную нормативную направленность: они нацелены на то, чтобы уточнить толкование уже существующих или предложить новые нормы международного права для регулирования деятельности, связанной с использованием ИКТ. Отличительной особенностью последних лет стало активное раскрытие самими государствами своей позиции по основным дискуссионным вопросам этой повестки. На национальном уровне свою позицию в стратегиях, концепциях и различных официальных заявлениях выразили Австралия[8], Великобритания[9], Израиль[10], Нидерланды[11], США [Koh 2012:1-12], Финляндия[12], Франция[13] и ФРГ[14]. В рамках работы Группы правительственных экспертов в 2021 г. по составлению компендиума своё мнение по вопросу применения

[3] ООН: Резолюция Генеральной Ассамблеи «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». 31.12.2020. Доступ: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement (дата обращения: 08.11.2021).

[4] ООН: Правила поведения в области обеспечения международной информационной безопасности. Приложение к письму постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций на имя Генерального секретаря. 12.09.2011. Доступ: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement (дата обращения: 08.11.2021); ООН: Правила поведения в области обеспечения международной информационной безопасности, Приложение к письму постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций. 09.01.2015. Доступ: https://daccess-ods.un.org/tmp/9398264.88494873.html (дата обращения: 08.11.2021).

[5] Convention on Cybercrime of 23 November 2001. URL: https://rm.coe.int/1680081561(accessed 08.11.2021); Arab Convention on Combating Information Technology Offences of 21 December 2010.
URL: https://unidir.org/cpp/en/multilateral-frameworks accessed 08.11.2021).

[6] В соответствии с анализом, проведённым Центром исследований в области международной безопасности (Университет Мэриленд), по состоянию на 2017 г. 196 подобных соглашений были заключены между 116 государствами [Hitchens, Goren 2017].

[7] ООН: Резолюция Генеральной Ассамблеи «Противодействие использованию информационно-коммуникационных технологий в преступных целя». 26.05.2021. Доступ: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/54/PDF/N2113354.pdf?OpenElement (дата обращения: 08.11.2021).

[8] Department of Foreign Affairs and Trade: Australia's International Cyber Engagement Strategy. Annex A: Australia's Position on the Application of International Law to State Conduct in Cyberspace. 2019. URL: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF (accessed 08.11.2021); Department of Foreign Affairs and Trade: Australia's International Cyber Engagement Strategy. Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace. 2017. URL: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf (accessed 08.11.2021).

[9] UK Attorney General's Office: Cyber and International Law in the 21st Century. The Attorney General Jeremy Wright QC MP Speech on the UK's Position on Applying International Law to Cyberspace. May 23, 2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (accessed 08.11.2021).

[10] 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-concerning-the-application-of-international-law-to-cyber-operations/ (accessed 08.11.2021).

[11] Ministry of Foreign Affairs (The Netherlands): Letter to the Parliament on the International Legal Order in Cyberspace. 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 08.11.2021). Далее – «Ministry of Foreign Affairs (The Netherlands)».

[12] Finland's National Positions. International Law and Cyberspace. 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyber-and-international-law-oct-2020.pdf (accessed 08.11.2021)

[13] Ministère des Armées (France): International Law Applied to Operations in Cyberspace. 2019. URL: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (accessed 08.11.2021). Далее – «Ministère des Armées (France)».

[14] Deutscher Bundestag: Krieg im „Cyber-Raum" – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung. 10.12.2015. S. 4-5, 7. URL: https://dserver.bundestag.de/btd/18/069/1806989.pdf (accessed 08.11.2021).

норм международного права к использованию ИКТ представили 15 государств[15]. Девять ответов поступило в процессе опроса, проведённого Организацией американских государств [Hollis 2020:5]. На фоне этих цифр однозначным прорывом стали заседания и подготовительная работа по составлению финального доклада первой Рабочей группы открытого состава: именно этот формат позволил услышать позицию большинства государств мира[16].

Однако можно ли сделать вывод о том, что все эти усилия привели к прояснению, по меньшей мере, ключевых вопросов, связанных с международно-правовой квалификацией вредоносного использования ИКТ? Данная статья призвана, учитывая как доклады Группы правительственных экспертов ООН и Рабочей группы открытого состава, так и официальные позиции отдельных государств, пролить свет на то, в какой степени и по каким вопросам применения первичных норм международного права для квалификации вредоносного использования ИКТ государствам удалось достичь консенсуса, поскольку именно он важен при выявлении как последующей практики применения международных договоров, которая устанавливает соглашение участников относительно их толкования[17], так и практики и *opinio juris,* как элементов новых международных обычаев[18].

2. Позиции государств в отношении распространения первичных норм международного права на случаи вредоносного использования ИКТ

Если обратиться к общим, не созданным специально для регулирования «киберсферы», нормам права, то вредоносное использование ИКТ, помимо уголовного законодательства отдельных государств, может нарушать принципы уважения суверенитета и невмешательства в дела других государств, запрет применять и угрожать применением силы, а также, в случае вооружённого конфликта, – нормы международного гуманитарного права. Гипотетически, эти деяния, могут нарушать и международное право прав человека, однако, учитывая лимиты экстерриториального применения соответствующих международных договоров, а также то, что многие из данных операций будут подпадать под понятие «шпионажа», который не запрещён международным правом, эта возможность достаточно ограничена. Обязанность проявлять надлежащую осмотрительность (*due diligence* – англ.), требующую от государств обеспечить, чтобы, как это сформулировано в Таллиннском руководстве 2017 г., «их территория не использовалась как база для государственных и негосударственных приводящих к серьёзным последствиям враждебных кибероперациий против другого государства» [Tallinn Manual… 2017:30-50], в части, выходящей за пределы общей обязанности государств «не позволять, чтобы их территория использовалась для совершения актов, посягающих на права других государств», как это было установлено Международным судом в деле *о канале Корфу*[19], до сих пор находится в зачаточной форме [Chircop 2018:667-668], и, несмотря на позицию некоторых государств[20], рассматривается как lex ferenda[21] [Shackelford, Russell, Kuehn 2016:22-23; Delerue 2020: 353-376; Jensen, Watts 2017:1573-1574]. Исходя из этих соображений, последующий анализ будет ограничен тремя основными блоками первичных норм

[15] ООН: Официальный сборник добровольно представляемых национальных материалов по вопросу о том, как международное право применяется к использованию информационно-коммуникационных технологий государствами, предоставленных участвующими правительственными экспертами, входящими в Группу правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, созданную в соответствии с резолюцией 73/266 Генеральной Ассамблеи. 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-RU.pdf (дата обращения: 08.11.2021). Далее – «Компендиум-2021».

[16] UN: Open-Ended Working Group. URL: https://www.un.org/disarmament/open-ended-working-group/ (accessed 08.11.2021).

[17] Пункт 3 (b) ст. 31 Венской конвенции о праве международных договоров от 23 мая 1969 г. – *Ведомости Верховного Совета СССР.* 10.09 1986. № 37. Ст. 772.

[18] Ст. 38 Статута Международного суда от 26 июня 1945 г. – *Действующее международное право*. Сост. Ю.М. Колосов, Э.С. Кривчикова. Т. 1. М. 1999. С. 797.

[19] International Court of Justice: Corfu Channel Case (UK v. Albania). Judgment of 9 April 1949. – *I.C.J. Reports.* 1949. P. 4.

[20] Ministry of Foreign Affairs (The Netherlands). P. 4-5; Ministère des Armées (France). P. 9-10.

[21] ООН: Записка Генерального секретаря «Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности». 22.06. 2015. § 13(c). Доступ: https://digitallibrary.un.org/record/799853/files/A_70_174-RU.pdf (дата обращения: 08.11.2021). Далее – «Доклад ГПЭ-2015».

международного права: во-первых, принципами уважения суверенитета и невмешательства во внутренние дела, во-вторых, правом международной безопасности, и, в-третьих, международным гуманитарным правом.

2.1. Принципы уважения суверенитета и невмешательства во внутренние дела

Отношение государств к применению в отношении случаев вредоносного использования ИКТ двух принципов международного права: принципа уважения суверенитета и невмешательства во внутренние дела – очень чётко отражает дихотомию между, с одной стороны, теми типами вмешательства, которые государства не хотят допускать в отношении себя, и, с другой стороны, теми, которые они хотели бы иметь возможность использовать в отношении других [Русинова 2018:41-49]. Это проявилось в двух основных моментах.

Во-первых, в отношении применения принципа невмешательства во внутренние дела вне рамок контекста ИКТ государства зарезервировали довольно высокую и сложно достижимую планку. Квинтэссенцией этого подхода является сформулированный Международным судом в деле *Никарагуа против США*[22] в 1986 г. двухзвенный тест. Он состоит в том, что принцип невмешательства будет нарушен, если, во-первых, вторжение «осуществляется в отношении вопросов, которые каждому государству разрешено, в силу принципа суверенного равенства, решать самостоятельно» (или «*domaine réservé*»)[23], и, во-вторых, при этом используются «методы принуждения в отношении того выбора, который должен оставаться свободным»[24]. Это сопоставимо с забрасыванием сети с очень широкими ячейками. Этот же подход применяется в отношении случаев использования ИКТ. Отсюда, принцип невмешательства, отличаясь ограниченностью сферы применения, в контексте применения ИКТ становится практически бесполезным. Это вытекает из того, что в большинстве случаев вредоносного использования ИКТ отсутствует элемент принуждения: нападения на компьютерные сети, которые имеют своей целью причинить ущерб, получить выкуп, отомстить за какие-либо действия или получить информацию, этому критерию не удовлетворяют. При этом некоторыми государствами предпринимаются попытки трактовать критерий «*domaine réservé*» как не только связанный с исполнением государством своих властных полномочий, а как «щит, покрывающий целые области политики»[25]. Это, прежде всего, связано с попыткой государств обезопасить себя от вмешательства в выборы. Насколько далеко может зайти такой подход видно на примере Норвегии, заявившей о том, что противоправным вмешательством во внутренние дела является «оказание ненадлежащего влияния на общественное мнение»[26]. Вместе с тем, пока такие попытки остаются единичными: если государства и выделяют вмешательство в выборы, то большинство из них всё равно указывает на необходимость применять к этому типу вмешательства общий двухзвенный тест[27].

В целом же, роль принципа невмешательства при оценке правомерности вредоносного использования ИКТ достаточно скромна, и на текущий момент, пожалуй, только вмешательство в выборы является единственным примером, иллюстрирующим попытки модифицировать сферу применения этого принципа. Отсюда, на первый план выходит вытекающий из принципа суверенного равенства государств принцип уважения суверенитета. Хотя этот принцип тесно связан с принципом невмешательства во внутренние дела, из решения Международного суда по делу *Никарагуа против США* следует, что их содержание не идентично, и принцип уважения территориального суверенитета может быть нарушен действиями, которые не квалифициру-

См. также: U.S. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. 2011. § 10. URL: obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 08.11.2021).

[22] 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. – *I.C.J. Reports.* 1986. P. 14. Para. 240. Далее – «Case concerning Military and Paramilitary Activities in and against Nicaragua».

[23] Ibidem.

[24] Ibidem.

[25] Ziegler K. S. Domaine Réservé – *The Max Planck Encyclopedia of Public International Law.* Vol. III. Ed. by R. Wolfrum. Oxford: Oxford University Press. 2012. P. 213.

[26] Компендиум-2021 (Норвегия). С. 69.

[27] Компендиум-2021 (Бразилия). С. 19.

ются в качестве нарушения принципа невмешательства. В частности, таким нарушением были признаны пролёты американских самолётов над территорией Никарагуа[28]. Однако общего теста проверки соблюдения этого принципа, в отличие от принципа невмешательства во внутренние дела, ни в практике государств, ни в доктрине выработано не было.

Отметим, что при составлении Таллиннского руководства мнения экспертов о нижней планке нарушения принципа уважения суверенитета и круге инфраструктурных объектов, подпадающих под его защиту, серьёзно разделились [Tallinn Manual…2017:20-27]. Однако раскол в мнениях государств оказался значительно глубже. США и Соединённое Королевство заявили о том, что принцип уважения суверенитета является «общим принципом», «одной из фундаментальных концепций международного права», но не нормой права[29], то есть этот принцип не является отдельной нормой, которая может быть нарушена, если использование ИКТ не может быть квалифицировано как нарушение принципа невмешательства во внутренние дела.

В ответ на это несколько государств вступились за нормативный характер принципа уважения суверенитета. При этом Нидерланды, Финляндия и Швейцария сослались на подход, отражённый в Таллиннском руководстве 2017 г., в соответствии с которым этот принцип будет нарушен в случае, если будет иметь место посягательство на территориальную целостность, узурпация или вмешательство в осуществление государственных функций[30], и подчеркнули необходимость применения минимальной планки[31]. Некоторые же государства – как, к примеру, Бразилия, Норвегия и Франция, – попытались зарезервировать максимально широкий подход к содержанию этого принципа. Как указало Министерство обороны Франции, суверенитет этого государства нарушает любая кибератака на, во-первых, «информационные системы, расположенные на её территории», включая «оборудование и инфраструктуру, находящиеся на её территории; связанные объекты, их компоненты»; во-вторых, кибератака на «контент, управляемый или передаваемый по каналам электронной коммуникации, находящимся на национальной территории, или исходящий с IP адресов, относящихся к Франции»; и, в-третьих, кибератака на национальные домены.[32] Схожую позицию представила Норвегия[33], а об очень широком подходе Бразилии можно судить по тому, что в качестве примера нарушения суверенитета она привела «перехват коммуникаций»[34].

Правовые позиции, основанные на отрицании или, наоборот, признании нормативности принципа уважения суверенитета, несмотря на кажущуюся несовместимость, не так далеки друг от друга: обе постулируют невозможность применить данный принцип без конкретизации его содержания в отношении использования ИКТ. Разница состоит лишь в том, что в первом случае этот вывод эксплицитен, в во втором – имплицитен, так как многообразие подходов к содержанию принципа уважения суверенитета, артикулированных настаивающими на нормативности данного принципа государствами, в конечном счёте свидетельствует об отсутствии самого правила, которое могло бы применяться в отно-

[28] Case concerning Military and Paramilitary Activities in and against Nicaragua. Paras. 251, 292.

[29] Chatham House: The Application of International Law to State Cyberattacks Sovereignty and Non-Intervention. Research Paper. 2019. URL: www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf (accessed 08.11.2021); UK Attorney General's Office: Cyber and International Law in the 21st Century. The Attorney General Jeremy Wright QC MP Speech on the UK's Position on Applying International Law to Cyberspace. May 23, 2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (accessed 08.11.2021); Компендиум-2021 (Соединённое Королевство). С. 117. § 10.

[30] Компендиум-2021 (Нидерланды). С. 56-57; Компендиум-2021 (Швейцария). С. 87; Finland's National Positions, International Law and Cyberspace. 2020. P. 2-3.

[31] Ministry of Foreign Affairs (The Netherlands): Letter to the Parliament on the International Legal Order in Cyberspace. 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 08.11.2021); Schmitt M. The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis. 2019. URL: www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis (accessed 08.11.2021); Finland's National Positions. International Law and Cyberspace. 2020. URL: front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyber-and-international-law-oct-2020.pdf (accessed 08.11.2021).

[32] Ministère des Armées (France). P. 9-10.

[33] Компендиум-2021 (Норвегия). С. 68.

[34] Компендиум-2021 (Бразилия). С. 18.

шении ИКТ. Однако полифоничность позиций государств не предвещает возможности достичь консенсус по этому вопросу в обозримом будущем.

2.2. Право международной безопасности

Применение норм *jus ad bellum,* касающихся правомерности использования силы в международных отношениях, основано на двусоставном подходе, вытекающем из Устава ООН, в соответствии с которым различаются понятия «применение силы» (п. 4 ст. 2) и «вооружённое нападение» (ст. 51)[35]. Этот подход был конкретизирован Международным судом как основанный на применении разных минимальных планок интенсивности, в зависимости от «размаха и последствий» использования силы[36]. Готовность большинства государств квалифицировать случаи вредоносного использования ИКТ как «применение силы» или даже «вооружённое нападение» даже вне рамок вооружённого конфликта свидетельствует не столько об увлечении, сколько о злоупотреблении «военной парадигмой» оценки этих деяний. Этот вывод основан на трёх посылках: во-первых, постоянно эксплуатируемом аргументе о неопределённости минимальной планки как понятия «применение силы», так и «вооружённое нападение», во-вторых, на применении аналогии с кинетическими нападениями, и, наконец, в-третьих, на допущении использования длинных цепочек причинно-следственной связи [Corten 2012:5-27].

Устоявшееся толкование норм *jus ad bellum* действительно исходит из того, что запрет применения силы может быть нарушен, вне зависимости от типа оружия[37], и имеет в своей основе причинно-следственную связь между применением силы и наступившими последствиями. Соответственно, поражающей силой оружия может быть и не кинетическое, а, к примеру, химическое или бактериологическое, воздействие, и в силу того, что последствия его применения сопоставимы с кинетическим (причинение смерти, повреждение здоровья, разрушение объектов), применение такого оружия будет подпадать под понятие «применение силы» или «вооружённое нападение» по Уставу ООН[38]. В случае с использованием ИКТ, однако, цепочка последствий может быть существенно длиннее по сравнению с традиционным использованием оружия. С одной стороны, было бы неверным отрицать, что некоторые типы вредоносного использования компьютерных программ могут принимать военную форму и будет корректным давать им правовую оценку с позиции j*us ad bellum.* С другой же, применяя аналогию в длинных цепочках причинно-следственной связи, легко пересечь ту грань, когда результаты применения аналогии между использованием ИКТ и кинетическими операциями будут прямо противоречить консенсусу государств о толковании объёма понятия «применение силы» как не охватывающего невоенные формы воздействия – такие, как, к примеру, «экономическое принуждение» [The Charter… 2002:118].

Вместе с тем, позиции, артикулированные членами Рабочей группы открытого состава в 2019-2020 г., только подтверждают то, что проведение аналогии между применением ИКТ и кинетическими операциями является мэйнстримом[39]. Только четыре государства выразили свои сомнения и обеспокоенность в этой связи. Бра-

[35] Пункт 4 ст. 2, ст. 51 Устава ООН; Case concerning Military and Paramilitary Activities in and against Nicaragua. § 191.

[36] Ibid. § 195.

[37] International Court of Justice: Legality of the Threat or Use of Nuclear Weapons. Advisory Opinion of 8 July 1996. – *I.C.J. Reports.* 1996. P. 226. § 39.

[38] Ibid.

[39] Open-Ended Working Group (OEWG): Second substantive session. 2020. URL: https://dig.watch/events/open-ended-working-group-oewg-second-substantive-session (accessed 08.11.2021); 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. URL: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF (accessed 08.11.2021); Department of Foreign Affairs and Trade: Australia's Cyber Engagement Strategy. Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace. 2017. URL: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf (accessed 08.11.2021); Federal Government (Germany): On the Application of International Law in Cyberspace. Position Paper. 2021. P. 5-6. URL: www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf (accessed 08.11.2021); UK Attorney General's Office: Cyber and International Law in the 21st Century. The Attorney General Jeremy Wright QC MP Speech on the UK's Position on Applying International Law to Cyberspace. May 23, 2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (accessed 08.11.2021), а также [Koh 2012:1-12].

зилия и Индия подчеркнули отсутствие ясности в отношении минимальной планки для понятий «применение силы» и «вооружённое нападение», в то время как Пакистан в общем выразил обеспокоенность применимостью ст. 51 Устава ООН к «кибероперациям». Россия заняла самую жёсткую позицию, заявив, что понятия «применение силы» и «вооружённое нападение» могут применяться только в контексте вооружённого конфликта, а кибернападение вне этого контекста под них не подпадает[40].

Однако, даже если не оспаривать корректность подхода, основанного на аналогии и причинно-следственной связи, многие из известных случаев вредоносного использования ИКТ[41] не будут подпадать даже под понятие «применение силы» из-за низкой интенсивности (размаха и прямых последствий) [Watts 2015:249–250]. Это серьёзное ограничение на пути применения «военной парадигмы», которое служит объяснением желания ряда государств за счёт формулирования своей позиции на национальном уровне повлиять на становление общего подхода к тому, где именно будут располагаться минимальные планки «применения силы» и «вооружённого нападения» в контексте использования ИКТ, и, в частности, сделать их предельно низкими.

Так, Франция установила, что даже «кибероперация без физических последствий» может быть квалифицирована как применение силы и разработала – отметим – неисчерпывающий список критериев, которые должны применяться при такой оценке. Среди них указаны: «происхождение операции и природа исполнителей (военная или нет), размах вмешательства, текущие или предполагаемые последствия операции или природа предполагаемой цели»[42]. Министр иностранных дел Нидерландов также заявил, что «нельзя исключать, что кибероперация с очень серьёзными финансовыми или экономическими последствиями может быть квалифицирована как применение силы»[43]. Наконец, разработанное в Великобритании «Руководство по кибероперациям» хотя и признаёт необходимость операции причинить «такие же или сопоставимые последствия, что и кинетическое нападение», чтобы подпадать под понятие «применение силы» по п. 4 ст. 2 Устава ООН, в сноске уточняет, что в качестве таковых могут квалифицироваться, например, «продолжительные нападения на банковскую систему Великобритании, которые могут нанести серьёзный финансовый ущерб государству, приведя к ухудшению экономической безопасности населения»[44]. Один из самых широких подходов к определению круга деяний, подпадающих под «применение силы», демонстрирует и позиция, озвученная Норвегией[45]. Представляется, что тем самым государства настолько далеко отходят от нормативного содержания понятий «применение силы» и «вооружённое нападение», что отстаивание данных подходов приобретает ограниченный юридический потенциал, и, скорее, носит политический характер, выполняя функцию сдерживания потенциальных угроз.

2.3. Международное гуманитарное право

Если распространение Устава ООН на случаи использования ИКТ было подтверждено Группой правительственных экспертов ещё в 2015 г., последним бастионом, по поводу которого велись споры, оставалось международное гуманитарное право. В докладе 2015 г. были отмечены только четыре принципа: гуманности, необходимости, пропорциональности и различия, – а итоговые доклады в 2016-2017 гг. вообще не были приняты Группой правительственных экспертов, в том числе из-за этих разногласий. В докладе 2021 г., наконец, была признала применимость «норм международного гуманитарного права», но шестая Группа сделала при этом важное уточнение о том, что они применимы только в ситуациях вооружённых конфликтов[46]. Отсю-

[40] Open-Ended Working Group (OEWG): Second substantive session. 2020. URL: https://dig.watch/events/open-ended-working-group-oewg-second-substantive-session (accessed 08.11.2021).

[41] Center for Strategic and International Studies, Significant Cyber Incidents Since 2006. URL: csis-website-prod.s3.amazonaws.com/s3fs-public/200901_Significant_Cyber_Events_List.pdf (accessed 08.11.2021).

[42] Ministère des Armées (France). P.7.

[43] Ministry of Foreign Affairs (The Netherlands). P. 4.

[44] UK Ministry of Defense: Cyber Primer (2nd ed. 2016). Annex 1A – International Law Aspects. P. 12. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf (accessed 08.11.2021)/

[45] Компендиум-2021 (Норвегия). С. 70.

[46] ООН: Записка Генерального секретаря «Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности. 14.07.2021.

да, признание получилось амбивалентным: хотя вместо отдельных принципов было указано на нормы международного гуманитарного права, вопрос о том, может ли сама по себе операция с использованием ИКТ квалифицироваться в качестве «вооружённого конфликта», так и остался за скобками, и, соответственно, как вызывал, так и с необходимостью будет вызывать разночтения в будущем.

Большинство государств в целом подтвердили применимость международного гуманитарного права (*jus in bello*) к операциям с использованием ИКТ. Аргумент оппонентов, среди которых Китай, Куба, Пакистан, Россия, а также Сирийская Арабская Республика[47], состоит том, что применимость международного гуманитарного права будет легитимировать милитаризацию «киберпространства». Если рассматривать и трактовать данный довод поверхностно, он может показаться идущим вразрез со всей историей развития норм *jus in bello.* Однако, этот аргумент может также означать, что к злоупотреблению «военной парадигмой» может привести отсутствие чёткого водораздела между, с одной стороны, «военным» использованием ИКТ, которое может квалифицироваться как «применение силы» или «вооружённое нападение» в соответствии с *jus ad bellum,* или подпадать под понятия «нападение» или «военная операция» в соответствии с *jus in bello,* и, с другой стороны, «невоенным» использованием ИКТ – деянием в сфере компьютерной информации, за которое по национальному праву может устанавливаться уголовная ответственность, и которое может совершаться, в том числе, и на фоне вооружённого конфликта. Таким образом, квалификация по *jus in bello* будет вытеснять «правоохранительную парадигму» квалификации: применение международного права прав человека или национального уголовного права, которое, в свою очередь, вполне может быть основано на международных договорах, посвящённых криминализации вредоносных деяний с использованием ИКТ.

Кроме того, нельзя упускать из виду то, что понятийный аппарат международного гуманитарного права в ряде случаев не приспособлен и не позволяет использовать нормы этой отрасли в отношении деяний, совершаемых в отношении компьютерного кода. Отсюда, коллективное подтверждение применимости международного гуманитарного права в этой сфере может либо привести к разочарованию, когда дальше общих принципов и классификации лиц возможность применить нормы международного гуманитарного права не зайдёт, либо начнёт подогревать желание растянуть существующие международно-правовые понятия и концепции так, чтобы они стали вмещать в себя и использование ИКТ. Действительно, можно идентифицировать, по меньшей меры, три области, где применение международного гуманитарного права к сфере ИКТ может быть исключительно проблематично.

Во-первых, если не растягивать понятие «нападение» по международному гуманитарному праву на вредоносную деятельность с использованием ИКТ, то встанет вопрос о недостаточности норм этой отрасли. Это вытекает из лаконичности положений *jus in bello,* посвящённых «военным операциям», причём, даже в случае вооружённого конфликта международного характера (в отношении конфликтов немеждународного характера такие положения вообще отсутствуют). При этом большинство случаев

§ 71(f). Доступ: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030R-1.pdf (дата обращения: 08.11.2021).

[47] 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. June 23, 2017. URL: https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf (accessed 08.11.2021); Министерство иностранных дел РФ: Ответ спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских на вопрос информагентства ТАСС о состоянии международного диалога в этой сфере. 29.06.2017. Доступ: http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288 (дата обращения: 08.1111.2021); о позиции КНР см.: 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 08. 11.2021); Open-Ended Working Group (OEWG): First substantive session. 2019. URL: https://dig.watch/events/open-ended-working-group-oewg-first-substantive-session#:~:text=from%20the%20meeting-,The%20first%20substantive%20session%20of%20the%20Open%2DEnded%20Working%20Group,RES%2F73%2F27) (accessed 08.11.2021); Open-Ended Working Group (OEWG): Second substantive session. 2020. URL: https://dig.watch/events/open-ended-working-group-oewg-second-substantive-session (accessed 08.11.2021).

вредоносного использования ИКТ не будут подпадать под достаточно детально урегулированные «нападения», и, соответственно, в лучшем случае, смогут быть квалифицированы как «военные операции». В соответствии с п. 1 ст. 51 и п. 1 ст. 57 Первого дополнительного протокола к Женевским конвенциям 1949 г. о защите жертв вооружённых конфликтов международного характера, обязанности сторон конфликта установлены слишком общó и ограничиваются возложением обязанности предоставлять «общую защиту» гражданскому населению «от опасностей, возникающих в связи с военными операциями», а также «проявлять заботу о том, чтобы щадить гражданское население, гражданских лиц и гражданские объекты».

Ограниченность применимости категории «нападение» по международному гуманитарному праву к операциям с использованием ИКТ нашла своё отражение в позиции Франции. Напомним, что Министерством обороны этого государства был заявлен очень широкий подход к тому, что можно считать «применением силы» по *jus ad bellum,* когда в качестве такового рассматривались операции, которые не причиняют физического ущерба. Тем не менее, зеркально перерастягивать категорию «нападение» по *jus in bello* Министерство обороны не стало, и, как результат, было вынуждено признать, что «большинство операций, включая наступательные кибероперации, проведённые Францией в ситуации вооружённого конфликта, не достигают минимальной планки нападения», соответственно, «они остаются урегулированными общими принципами международного гуманитарного права».[48]

Во-вторых, проблема возникает при попытке государств обойти ограничения понятия «нападение» по *jus in bello,* растягивая его объём так, чтобы он мог включать как можно больше видов вредоносного использования ИКТ. Например, юридический советник США Б. Эган отметил, что хотя «не все кибероперации достигают уровня “нападения” как правовой категории по праву международных вооружённых конфликтов», тем не менее, существует возможность квалифицировать такие операции как «нападения», «учитывая, среди прочего, приводит ли эта кибердеятельность к кинетическим или некинетическим последствиям, природу и охват этих последствий, а также сущность связи между такой деятельностью и конкретным вооружённым конфликтом»[49]. Применение такого подхода может привести к объективной неприменимости норм международного гуманитарного права, посвящённых «нападениям», к случаям вредоносного использования ИКТ, потому что эти правила задумывались и были сформулированы так, чтобы регулировать кинетические операции.

Третья проблема, связанная с применимостью международного гуманитарного права к вредоносному использованию ИКТ, проистекает из того факта, что исполнители могут состоять в различной степени связи с государственной или негосударственной стороной вооружённого конфликта. В совокупности с особой природой самой деятельности в сфере ИКТ, это обстоятельство может привести к тому, что ключевая для международного гуманитарного права категория «непосредственного участия в военных действиях», – в различных вариантах прочтения, представленных в правовой литературе [Interpretive Guidance…2009:46-64] и судебных решениях[50], – окажется недостаточно широкой. К такому результату может привести как требование о наличии тесной связи со стороной конфликта для целей классификации в качестве комбатанта или члена организованных вооружённых сил или группы, так и требования о причинении кинетического или схожего с кинетическим ущерба, прямой причинно-следственной связи и существовании связи с военными действиями.

3. Туманные перспективы правотворческого трека: стандарты вместо норм

Несмотря на большое количество проблем, с которыми сталкивается применение общих норм международного права *lex lata* к вредоносной деятельности с использованием ИКТ, правотворческий трек до сих пор не играет решающей роли. Сами государства, по крайней мере,

[48] Ministère des Armées.P.13.

[49] 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 08.11.2021).

[50] Supreme Court of Israel: The Public Committee against Torture in Israel v. the Government of Israel et al. Judgment of 13 December 2006. § 39. URL: http://elyon1.court.gov.il/Files_ENG/02/690/007/a34/02007690.a34.htm (accessed 08.11.2021).

их подавляющее большинство предпочитают не связывать себя какими-либо новыми обязательствами [Delerue 2019:315-316]. В качестве причин такого отношения публично озвучены: достаточность существующей «стратегической рамки» для регулирования «киберпространства» (Европейский Союз, Португалия), опасность того, что создание новых юридически обязательных норм будет размывать или создавать неопределённость в отношении уже существующих (Болгария, Италия), недостаточность практики государств (Израиль) или консенсуса между государствами (Великобритания), а также медлительность международного нормотворческого процесса по сравнению со скоростью развития технологий (США, Сингапур, Великобритания, Австралия). Только небольшое число государств указывают на предпочтительность правотворческого трека (Алжир, Нигерия, Россия, Сирия, КАРИКОМ), при этом, однако, некоторые из них дополнительно отмечают, что рассматривают необходимость создания новых норм исключительно в средне- или долгосрочной перспективе (ЮАР, Чили, Бразилия). Выработка новых договорных норм международного права пока ограничивается развитием сотрудничества государств в области борьбы с преступностью в области компьютерной информации[51].

Магистральную позицию занял основанный на консенсусе процесс формулирования «стандартов». Однако, если мы рассмотрим содержание стандартов, которые были одобрены Генеральной Ассамблеей ООН, то ни в их первоначальном виде (11 «добровольных и необязательных норм ответственного поведения государств»)[52], ни в их расширенном варианте (14 «норм поведения»)[53], они не привнесли какой-либо «добавленной стоимости» к оценке правомерности вредоносного использования ИКТ по сравнению с существующими нормами[54]. Каждый стандарт, который сформулирован как применимый к этой оценке, обязательно ограничен отсылкой на действующие нормы международного права; кроме того, ко всем «нормам ответственного поведения поведения» применима общая оговорка о том, что они «не предусматривают ограничения или запрета действий, согласующихся с нормами международного права»[55]. Подход, заключающийся в формулировании стандартов, может быть важен и вполне оправдан в качестве политического инструмента для того, чтобы дополнительно подтвердить применимость международного права к деятельности, связанной с использованием ИКТ [Akande, Coco, de Souza Dias 2022:34]. Тем не менее, «нормы ответственного поведения» по своему содержанию юридически тавтологичны, так как не добавляют ничего нового к оценке правомерности вредоносного использования ИКТ.

4. Заключение

Артикуляция государствами своих позиций о том, как именно нормы международного права должны применяться к вредоносным операциям с использованием ИКТ, свидетельствует о том, что менеджериализм постепенно отступает, уступая место консенсуализму. Однако, как показывает анализ озвученных государствами подходов, консенсус сложился на очень высоком уровне абстракции и вряд ли выходит за пределы признания распространения сферы действия общих норм международного права на ИКТ. Это закрепляет неопределённость в качестве ключевой характеристики международно-правовой оценки соответствующих случаев и делает практически любое суждение о нюансах применения норм международного права в «киберсфере» вы-

[51] См.: Министерство иностранных дел РФ: Интервью директора Департамента международной информационной безопасности МИД России А.В. Крутских «Глобальная киберповестка: дипломатическая победа» журналу «Международная жизнь». 07.06. 2021. Доступ: https://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/4778945 (дата обращения: 08.11.2021).

[52] Доклад ГПЭ-2015. § 13.

[53] ООН: Резолюция Генеральной Ассамблеи «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». 05.12.2018. Доступ: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement (дата обращения: 08.11.2021).

[54] Примечательно, что в ходе заседаний Рабочей группы открытого состава только Египет прямо высказался за трансформацию правил ответственного поведения, разработанных ГПЭ, в юридически-обязательные нормы; Филиппины выразили сожаление о необязательном характере данных рекомендаций и ограниченных возможностях по их имплементации.

[55] Доклад ГПЭ–2015. § 10.

водом *ad hoc* – волюнтаристским и оспоримым. Возможно, именно это обстоятельство объясняет то, что государства, реагируя на случаи вредоносного использования ИКТ, предпочитают выбирать политическую, а не юридическую риторику, а, если и обращаются к праву, то используют национальные нормы, связанные с применением мер принуждения (т.н. «санкции»[56]), как в случае с США, или наднациональные, как в случае с Европейским союзом. Использование этого трека [Roscini 2015:248-254] позволяет государствам обойти большинство ограничений и сложностей, связанных с применением как первичных норм международного права, так и вторичных норм, требующих соблюдения признанных в международном праве стандартов доказывания и раскрытия доказательств.

Список литературы

1. Ромашкина Н. П. 2020. Проблема международной информационной безопасности в ООН. – *Мировая экономика и международные отношения*. № 64. С. 25-32. DOI: 10.20542/0131-2227-2020-64-12-25-32
2. Русинова В. Н. 2018. Международно-правовой принцип невмешательства и кибероперации: неоправданные ожидания?. – *Международное правосудие*. № 1. С. 38-52. DOI: 10.21128/2226-2059-2018-1-38-52
3. 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.
4. Chircop L. 2018. A Due Diligence Standard of Attribution in Cyberspace. – *International and Comparative Law Quarterly*. Vol. 67. Issue 3. P. 643-668. DOI: 10.1017/S0020589318000015
5. Corten O. 2012. *The Law against War: The Prohibition on the Use of Force in Contemporary International Law*. Oxford; Portland: Hart Publishing. 569 p.
6. Delerue F. 2019. Reinterpretation or Contestation of International Law in Cyberspace?. – Israel Law Review. Vol. 52. Issue 3. P. 295-326. DOI:10.1017/S0021223719000104
7. Delerue F. 2020. *Cyber Operations and International Law*. Cambridge: Cambridge University Press. 513 p. DOI: https://doi.org/10.1017/9781108780605
8. Hitchens Th., Goren N. 2017. *International Cybersecurity Information Sharing Agreements. University of Maryland*. 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).
9. 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+State+Cyber+Operations_+Fourth+Report.pdf (accessed 01.11.2021).
10. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*. Ed. by N. Melzer. 2009. 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).
11. 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.
12. 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(accessed 01.11.2021).
13. Roscini M. 2015. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. – *Texas International Law Journal*. Vol. 50. Issue 2. P. 233-273.
14. 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.
15. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Ed. by M. N. Schmitt. 2017. Cambridge: Cambridge University Press. 598 p.
16. *The Charter of the United Nations. A Commentary*. Ed. by B. Simma. 2nd ed. 2002. – Oxford: Oxford University Press. 895 p.
17. Watts S. 2015. Low-Intensity Cyber Operations and the Principle of Non-Intervention. – *Cyber War: Law and Ethics for Virtual Conflicts*. Ed. by Ohlin J.D., Govern K., Finkelstein C. Oxford: Oxford University Press. P. 249–270. DOI: 10.1093/acprof:oso/9780198717492.003.0012

References

1. Akande D., Coco A., de Souza Dias T. Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies. – *International Law Studies*. 2022. Vol. 99. P. 4-36.
2. Chircop L. A Due Diligence Standard of Attribution in Cyberspace. – *International and Comparative Law Quarterly*. 2018. Vol. 67. Issue 3. P. 643-668. DOI: 10.1017/S0020589318000015

[56] Этот термин используется в международном праве в значении мер принудительного характера, которые принимает международная организация в соответствии со своими учредительными документами; соответственно, использование этого термина в национальном праве гораздо шире и охватывает все меры принуждения, которые призваны оказать давление на зарубежное государство, причём их правомерность не ставится в зависимость от совершения этим государством именно международно-противоправного деяния.

3. Corten O. *The Law against War: The Prohibition on the Use of Force in Contemporary International Law.* Oxford; Portland: Hart Publishing. 2012. 569 p.
4. Delerue F. 2019. Reinterpretation or Contestation of International Law in Cyberspace?. – Israel Law Review. Vol. 52. Issue 3. P. 295-326. DOI:10.1017/S0021223719000104
5. Delerue F. *Cyber Operations and International Law.* Cambridge: Cambridge University Press. 2020. 513 p. DOI: https://doi.org/10.1017/9781108780605
6. Hitchens Th., Goren N. *International Cybersecurity Information Sharing Agreements.* 2017. 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).
7. Hollis D. *Improving Transparency. International Law and State Cyber Operations. Fourth report to the Organization of American States.* 2020. 22 p. URL: https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Improving+Transparency+International+Law+and+State+Cyber+Operations_+Fourth+Report.pdf (accessed 01.11.2021).
8. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law.* Ed. by N. Melzer. Geneva: International Committee of the Red Cross. 2009. 89 p. URL: www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf (accessed 01.11.2021).
9. Jensen E.T., Watts S. A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?. – *Texas Law Review.* 2017. Vol. 95. P. 1555-1577.
10. Koh H.H. International Law in Cyberspace. – *Harvard International Law Journal Online.* 2012. Vol. 54. P. 1-12. URL: https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf (accessed 01.11.2021).
11. Romashkina N. P. Problema mezhdunarodnoi informatsionnoi bezopasnosti v OON [Problem of International Information Security in the UN]. – *Mirovaya ekonomika i mezhdunarodnye otnosheniya.* 2020. No.64. P. 25-32. (In Russ.). DOI: 10.20542/0131-2227-2020-64-12-25-32
12. Roscini M. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. – *Texas International Law Journal.* 2015. Vol. 50. Issue 2. P. 233-273.
13. Rusinova V. N. Mezhdunarodno-pravovoi printsip nevmeshatel'stva i kiberoperatsii: neopravdannye ozhidaniya? [The international legal principle of non-interference and cyber-operations: unjustified expectations?]. – *Mezhdunarodnoe pravosudie.* 2018. No. 1. P. 38-52. (In Russ.) DOI: 10.21128/2226-2059-2018-1-38-52
14. Shackelford S.J., Russell S., Kuehn A. Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors. – *Chicago Journal of International Law.* 2016. Vol. 17. P. 1-51.
15. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Ed. by M. N. Schmitt. Cambridge: Cambridge University Press. 2017. 598 p.
16. *The Charter of the United Nations. A Commentary.* Ed. by B. Simma. 2nd ed. Oxford: Oxford University Press. 2002. 895 p.
17. Watts S. Low-Intensity Cyber Operations and the Principle of Non-Intervention. – *Cyber War: Law and Ethics for Virtual Conflicts.* Ed. by Ohlin J.D., Govern K., Finkelstein C. Oxford: Oxford University Press. 2015. P. 249–270. DOI: 10.1093/acprof:oso/9780198717492.003.0012

Информация об авторе

Вера Николаевна Русинова,
доктор юридических наук, профессор, руководитель департамента международного права, Факультет права, Национальный исследовательский университет «Высшая школа экономики»

101000, Российская Федерация, Москва, ул. Мясницкая, д. 20

vrusinova@hse.ru
ORCID: 0000-0002-5838-0283

About the Author

Vera N. Rusinova,
Doctor of Juridical Sciences, 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

vrusinova@hse.ru
ORCID: 0000-0002-5838-0283