Vestnik RUDN. International Relations. ISSN 2313-0660 (Print), ISSN 2313-0679 (Online) 2026 Vol. 26 No. 1 62–76
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ http://journals.rudn.ru/international-relations

DOI: 10.22363/2313-0660-2026-26-1-62-76
EDN: TCJXVU

Обзорная статья / Review article

Проблема применимости международного гуманитарного права к кибероперациям: обзор российского и западных подходов

В.Б. Козюлин

Дипломатическая академия МИД РФ, Москва, Российская Федерация
✉ v.kozyulin@dipacademy.ru

Аннотация. Актуальность темы исследования обусловлена тем, что кибероперации становятся неотъемлемым элементом современных вооруженных конфликтов, при этом применимость международного гуманитарного права (МГП) к цифровой среде остается дискуссионной. На практике это проявляется в отсутствии устоявшихся критериев, позволяющих однозначно отнести конкретное кибервоздействие к «нападению», «использованию силы» или к недружественным, но формально правомерным действиям. В условиях трансграничности информационно-коммуникационных технологий (ИКТ), анонимности действий и вовлечения негосударственных акторов отсутствует единый подход к квалификации кибердеяний и защите гражданской инфраструктуры, что затрудняет выработку согласованной международной реакции на киберинциденты. Дополнительную сложность создает то, что значительная часть кибероперaций не приводит к физическому разрушению, а выражается в потере функциональности систем, что ставит под вопрос традиционные представления о насилии и ущербе в МГП. Методологически исследование опирается на сравнительно-правовой анализ официальных национальных позиций, документов ООН и специализированных доктринальных источников, а также на системное толкование норм МГП применительно к новым видам вооруженного противоборства. Используются методы юридико-догматического анализа, контент-анализ государственных доктрин и экспертных комментариев, а также элементы кейс-стади в части рассмотрения типичных киберинцидентов, включая операции против объектов критической инфраструктуры и информационных систем двойного назначения. Научная новизна исследования состоит в комплексном раскрытии трех узловых аспектов применения МГП к кибероперациям: цифрового суверенитета, квалификации кибератак и разграничения военных и гражданских целей в киберпространстве. Впервые в единой рамке сопоставлены российский и западные подходы к понятию суверенитета в цифровой среде, к порогам отнесения кибервоздействий к «нападению», а также к статусу данных и объектов двойного назначения в контексте гуманитарной защиты. Полученные результаты показывают, что разнородность национальных подходов к цифровому суверенитету создает препятствия для выработки согласованных критериев применения принципов различения, соразмерности и предосторожности к кибероперациям, не сопровождающимся физическим разрушением. Обоснована необходимость уточнения статуса данных как объектов защиты по МГП и адаптации традиционных категорий военных и гражданских целей к условиям функционирования критической информационной инфраструктуры.

Ключевые слова: информационно-коммуникационные технологии, информационное право, цифровой суверенитет, кибервойна, международная безопасность, критическая инфраструктура, гуманитарная защита, атрибуция киберинцидентов, гражданское население, двойное назначение, правовой режим данных

Заявление о конфликте интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: *Козюлин В.Б.* Проблема применимости международного гуманитарного права к кибероперациям: обзор российского и западных подходов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2026. Т. 26, № 1. С. 62–76. https://doi.org/10.22363/2313-0660-2026-26-1-62-76; EDN: TCJXVU

The Applicability of International Humanitarian Law to Cyber Operations: A Review of Russian and Western Approaches

Vadim B. Kozyulin

Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, Moscow, Russian Federation

✉ v.kozyulin@dipacademy.ru

Abstract. The relevance of this study stems from the fact that cyber operations have become an integral element of contemporary armed conflicts, while the applicability of international humanitarian law (IHL) to the digital environment remains contested and is only partially regulated. In practice, this is reflected by the lack of well-established criteria for classifying specific cyber operations as an "attack," a "use of force," or as unfriendly yet formally lawful conduct. Given the transboundary nature of information and communication technologies, the anonymity of actors, and the involvement of non-state entities, there is still no common approach to qualifying cyber activities or protecting civilian infrastructure, which complicates the development of a coordinated international response to cyber incidents. The problem is further exacerbated by the fact that many cyber operations do not cause physical destruction, but rather result in a loss of functionality of systems, calling into question traditional understandings of violence and harm under IHL. The methodology of the study combines a comparative legal analysis of official national positions, United Nations documents, and specialized doctrinal sources, with a systematic interpretation of IHL norms as applied to new forms of armed confrontation. The research employs doctrinal legal analysis, content analysis of governmental doctrines and expert commentaries, as well as elements of case studies focusing on representative cyber incidents, including operations targeting critical infrastructure and dual-use information systems. This article contributes to the literature by providing an integrated examination of three pivotal dimensions of the application of IHL to cyber operations: digital sovereignty, the classification of cyber-attacks, and the distinction between military and civilian objectives in cyberspace. For the first time within a single analytical framework, it juxtaposes Russian and Western approaches to sovereignty in the digital domain, to the thresholds for qualifying cyber activities as "attacks," and to the legal status of data and dual-use objects for humanitarian protection purposes. The findings demonstrate that divergent national approaches to digital sovereignty and attribution impede the development of common criteria for applying the IHL principles of distinction, proportionality and precaution to cyber operations that do not involve physical destruction. The article therefore argues for clarifying the status of data as objects protected under IHL and for adapting traditional categories of military and civilian objectives to the operating conditions of critical information infrastructure.

Key words: information and communication technologies, information law, digital sovereignty, cyber warfare, international security, critical infrastructure, humanitarian protection, attribution of cyber incidents, civilian population, dual-use, legal regime of data

Conflicts of interest. The author declares no conflicts of interest.

For citation: Kozyulin, V.B. (2026). The applicability of international humanitarian law to cyber operations: A review of Russian and Western approaches. *Vestnik RUDN. International Relations*, 26(1), 62–76. https://doi.org/10.22363/2313-0660-2026-26-1-62-76; EDN: TCJXVU

Введение

Рассмотрение в ООН вопросов применения норм международного права, в том числе международного гуманитарного права (МГП) к кибероперациям показало, что достижение согласия остается сложной задачей. Западные страны полагают, что существующего международного права, и в частности МГП, достаточно для регулирования межгосударственного противоборства в сфере информационно-коммуникационных технологий (ИКТ), а кибертерроризм и киберпреступность надлежит рассматривать в пределах отдельной системы международного права (Schmitt, 2017a). В свою очередь Россия выступает за создание всеобъемлющего международного механизма регулирования применения международного права в области информационно-коммуникационных технологий под эгидой ООН, при этом особое внимание уделяется учету специфических особенностей цифровой среды, таких как возможность анонимности действий ее участников[1].

Россия, Китай, а также ряд их государств-партнеров и международных организаций полагают, что многие ключевые нормы международного гуманитарного права в настоящее время не находят практического применения к киберинцидентам и требуют дополнительного разъяснения[2].

Главные задачи данного исследования заключаются в рассмотрении возможности применения международного гуманитарного права к кибероперациям в условиях вооруженных конфликтов, а также в анализе возможностей модификации существующих международно-правовых механизмов для решения вопросов, возникающих в сфере кибервойны, таких как атрибуция, военная необходимость и разграничение военных и гражданских объектов.

Научная новизна исследования заключается во всестороннем рассмотрении применимости МГП к операциям в киберпространстве, относительно малоисследованной области юридической науки и международных отношений. В работе представлен критический анализ различных национальных точек зрения — в частности, западных стран и России — на толкование и применение МГП в киберпространстве, выявлены пробелы в существующей правовой базе и предложены области для дальнейшего развития этой сферы.

Методологически исследование опирается на общенаучные принципы системности, историзма и междисциплинарного подхода, предполагающие рассмотрение кибероперации как элемента эволюции вооруженных конфликтов и международно-правового регулирования. На этой базе используются специальные методы юридического анализа: сравнительно-правовой анализ национальных подходов к применению международного гуманитарного права в киберпространстве, а также доктринальный анализ профильной литературы и международных документов, позволяющие выявить расхождения в трактовке цифрового суверенитета, кибератак и статуса данных.

Западная школа применения МГП к кибероперациям

Основополагающим документом западной школы права в отношении регулирования киберпространства является Таллинское руководство, разработанное под руководством Центра передового опыта совместной кибербезопасности Организации Североатлантического договора (НАТО). Первое издание (2013) сосредоточилось на применении *jus ad bellum*

[1] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[2] Доклад Группы правительственных экспертов ООН по вопросам достижений в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/76/135 // ООН. 14.07.2021. URL: https://digitallibrary.un.org/record/3964709/files/DSS_33_Russian.pdf (дата обращения: 28.09.2025).

и *jus in bello* к кибероперациям, установив критерии квалификации «кибератаки» как акта насилия (Schmitt, 2013). Еще до появления Таллинское руководства Н. Мельцер в работе, подготовленной для Института ООН по исследованию проблем разоружения (ЮНИДИР), обозначил основные коллизии применения *jus ad bellum* и *jus in bello* к кибервойне, включая проблемы порога вооруженного конфликта и атрибуции (Melzer, 2011).

В статье Э.Т. Дженсена (Jensen, 2017) и в самом издании «Таллинское руководство 2.0 по международному праву, применимому к кибероперациям», автор и группа экспертов НАТО подробно раскрывают применимость норм *jus ad bellum* и *jus in bello* к кибероперациям, предлагая систему правил по вопросам суверенитета, должной осмотрительности, квалификации кибератак и защиты гражданских объектов (Schmitt, 2017b).

Эксперты под руководством М. Шмитта разработали детальную систему применения действующего международного права к кибероперациям, включая принципы различения, соразмерности и предосторожности (Schmitt, 2017b, pp. 54–68). Было расширено понятие «вооруженного нападения» на высокодеструктивные кибероперации и прояснило соотношение *jus ad bellum* и *jus in bello* в цифровой среде (Schmitt, 2017b). В более поздней работе М. Шмитт систематизировал эволюцию доктрины *jus ad bellum* применительно к киберпространству за прошедшее десятилетие, констатируя, что, несмотря на растущий консенсус по ряду вопросов, проблема «порога» вооруженного нападения остается нерешенной (Schmitt & Pakkam, 2024).

В монографии М. Роччини анализируется, в каких случаях кибероперации могут рассматриваться как «применение силы» или «вооруженное нападение» в контексте принципов Устава ООН и как нормы права вооруженных конфликтов регулируют выбор средств и методов кибервойны. Автор подробно рассматривает «пограничные» сценарии, когда кибервоздействие не приводит к физическому разрушению, но создает значительные функциональные последствия для критической инфраструктуры (Roscini, 2014, pp. 367–368).

Международный комитет Красного Креста (МККК) также активно развивает концепцию защиты гражданских объектов в киберпространстве[3]. МККК предложил инновационную идею «цифровой эмблемы» для защиты медицинских и гуманитарных организаций от кибератак[4]. Одним из первых системных исследований этой проблематики стала работа К. Дреге, в которой обосновывается необходимость распространения принципов защиты гражданского населения на операции в киберпространстве и анализируются пределы применимости норм *jus in bello* к кибератакам, не сопровождающимся физическим разрушением (Droege, 2012).

Особую роль в развитии гуманитарной оптики играют исследования юридического отдела МККК. В статье Л. Гизеля, Т. Роденхойзера и К. Дорманна обосновывается, что кибероперации в ходе вооруженных конфликтов однозначно подпадают под действие МГП, а ключевыми проблемами становятся критерии отнесения конкретных кибервоздействий к «нападениям» и вопрос о том, должны ли данные пользоваться защитой наравне с материальными гражданскими объектами (Gisel, Rodenhäuser & Dörmann, 2020).

Министерство обороны США подчеркивает, что принципы права войны применяются к кибероперациям независимо от формального статуса вооруженного конфликта. В выступлении Генерального юрисконсульта П.С. Нея подчеркивается, что последствия кибероперации должны оцениваться по их эквивалентности применению силы традиционными средствами, а также фиксируется обязанность соблюдать принципы различения, соразмерности и предосторожности при планировании и проведении

[3] International Humanitarian Law and Cyber Operations during Armed Conflicts // International Committee of the Red Cross. November 28, 2019. URL: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts (accessed: 28.09.2025).

[4] Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems // International Committee of the Red Cross. November 3, 2022. URL: https://www.icrc.org/en/document/icrc-digital-emblems-report (accessed: 28.09.2025).

военных кибероперацій[5]. Американский подход фокусируется на результате воздействия (функциональный ущерб, вывод из строя критической инфраструктуры), а не на конкретных технических средствах, что позволяет распространять существующие нормы МГП на широкий спектр кибердействий.

Нидерланды, Франция, Великобритания и Австралия признают применимость МГП к киберпространству с различными акцентами на толковании принципов суверенитета и невмешательства.

Нидерланды в парламентском письме 2019 г. представили развернутую позицию по применению международного права в киберпространстве, прямо признавая суверенитет самостоятельным обязательством, нарушение которого в результате кибероперацій может образовывать международно-противоправный акт. Голландский подход детально раскрывает вопросы допустимости контрмер, атрибуции и политической координации реакции на кибератаки, подчеркивая, что существующее международное право обеспечивает достаточную основу для регулирования поведения государств в цифровой среде[6].

Франция в своем «Заявлении о международном праве в киберпространстве» 2019 г. подтверждает применимость принципов суверенитета, невмешательства и запрета угрозы силой к кибероперациям и исходит из того, что любое кибервоздействие, нарушающее конфиденциальность, целостность или доступность французских информационных систем, при атрибуции другому государству является как минимум нарушением суверенитета Франции. Французская позиция подчеркивает, что право на контрмеры и самооборону в киберпространстве должно реализовываться строго в рамках международного права и исключает «ответные хакерские действия» частных компаний[7].

Великобритания в официальном заявлении 2021 г. подтверждает, что международное право в полной мере распространяется на деятельность государств в киберпространстве, но при этом выражает более сдержанную позицию в отношении суверенитета как самостоятельного основания ответственности, считая, что сам по себе принцип суверенитета не образует отдельного «запрета» для кибероперацій сверх норм о невмешательстве[8]. В речах Генерального атторнея (Дж. Райта в 2018 г.[9] и С. Браверман в 2022 г.[10]) проводится разграничение между кибероперациями, достигающими порога применения силы и вооруженного нападения, и иными недружественными, но менее масштабными кибервоздействиями.

В программном документе Австралии подчеркивается, что Устав ООН в целом, включая нормы о запрещении угрозы силой, самообороне и ответственности государств, полностью применим к кибероперациям, но при этом указываются новые вызовы, связанные

[5] Ney Jr. P.C. DoD General Counsel Remarks at U.S. Cyber Command Legal Conference // U.S. Department of War. March 2, 2020. URL: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference (accessed: 28.09.2025).

[6] Schmitt M. The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis // Just Security. October 14, 2019. URL: https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/ (accessed: 28.03.2025).

[7] Roguski P. France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I // Opinio Juris. September 24, 2019. URL: https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accessed: 28.09.2025).

[8] Application of International Law to States' Conduct in Cyberspace: UK Statement // Foreign, Commonwealth & Development Office. June 3, 2021. URL: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement (accessed: 28.09.2025).

[9] Speech: Cyber and International Law in the 21st Century // Gov.uk. May 23, 2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (accessed: 28.03.2025).

[10] Jowitt T. UK Can Legally Launch Cyberattacks Against Hostile Nations, Says AG // Silicon. May 19, 2022. URL: https://www.silicon.co.uk/e-regulation/governance/uk-legally-launch-cyberattacks-says-ag-458458 (accessed: 28.03.2025).

с суверенитетом, атрибуцией и юрисдикцией. Австралийская сторона прямо ссылается на нормы о международной ответственности государств и подчеркивает необходимость прозрачности национальных интерпретаций международного права в киберпространстве[11].

Таким образом, анализ позиций западных государств и международных организаций показывает, что, несмотря на широкое согласие относительно применимости существующего международного права и МГП к кибероперациям, сохраняются расхождения по вопросам содержания цифрового суверенитета, порогов квалификации кибератак как «использования силы» или «вооруженного нападения», а также процедур международно-правовой атрибуции. Требует дальнейшей проработки и проблема разграничения военных и гражданских целей в цифровой среде, включая правовой режим критической информационной инфраструктуры и данных как потенциальных объектов защиты в рамках МГП (Giovanelli, 2025).

Российские исследования

Российская научная школа представлена работами С.Ю. Гаркуши-Божко, исследующего проблемы *ratione materiae* (лат. «в силу предмета», «по причине существа дела») и *ratione temporis* (лат. «по причине времени», «в силу времени») применения МГП в киберпространстве. Автор отмечает существенные сложности в квалификации кибероперациий как актов вооруженного конфликта и подчеркивает необходимость более широкого понимания информационного противоборства. С.Ю. Гаркуша-Божко показывает, что отсутствие согласованного понимания «вооруженного нападения» и «кибератаки» приводит к разночтениям в вопросах законности применения силы и гуманитарной защиты (Гаркуша-Божко, 2021).

А.В. Коротков и Е.С. Зиновьева исследуют безопасность критических информационных инфраструктур в международном гуманитарном праве, обращая внимание на проблемы разграничения военных и гражданских целей в условиях двойного использования цифровых объектов (Коротков, Зиновьева, 2011).

Официальная позиция России изложена в комментариях к документам Рабочей группы открытого состава, подчеркивающих необходимость учета суверенных прав государств в информационном пространстве[12]. Российская дипломатия действует в соответствии с Указом Президента РФ от 12.04.2021 г. № 213, определяющим содействие совершенствованию под эгидой ООН принципов и норм МГП применительно к сфере ИКТ[13].

В статье «Международное право и война в киберпространстве» Г.Г. Шинкарецкая рассматривает проблемы применимости норм МГП к воздействиям на информационные и кибернетические системы и приходит к выводу, что базовые принципы МГП (различение, соразмерность, предосторожность) полностью сохраняют силу в киберпространстве, однако специальные нормы в отношении кибероружия и кибероперациий находятся в стадии формирования, что создает правовую неопределенность для государств (Шинкарецкая, 2013).

В более новой работе «Противодействие кибератакам: пробелы международного права и перспективы их преодоления» анализируются юридические последствия кибератак, сложности атрибуции и привлечения к ответственности,

[11] 2017 — Australia's Position on the Application of the International Law to State Conduct in Cyberspace // Department of Foreign Affairs and Trade. URL: https://www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf (accessed: 01.02.2025).

[12] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[13] Указ Президента Российской Федерации № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» от 12 апреля 2021 г. // Президент России. URL: http://www.kremlin.ru/acts/bank/46614 (дата обращения: 28.09.2025).

а также национальные и международные меры реагирования на киберугрозы. Авторы систематизируют существующие международно-правовые механизмы самообороны и коллективной безопасности в киберсфере и подчеркивают необходимость разработки специальных процедур и стандартов доказательств для международной атрибуции киберинцидентов (Рахман, Дас, 2024).

Цифровой суверенитет в контексте МГП

Концепция цифрового суверенитета предполагает право государства контролировать информационные потоки на своей территории и обеспечивать безопасность национального информационного пространства[14]. В контексте МГП данная концепция приобретает особое значение при определении юрисдикции и применимого к кибероперациям права.

Понятие «суверенитет» меняется, и если раньше оно распространялось на воздушное пространство и шельф, то сегодня формируется понятие «цифровой суверенитет», который представляет собой часть технологического суверенитета (суверенитет в области данных и цифровой инфраструктуры, в том числе критической).

Позиция России по цифровому суверенитету

Россия последовательно отстаивает принцип информационного суверенитета государств[15]. В документах, представленных для Рабочей группы открытого состава, подчеркивается «суверенное право каждого государства на обеспечение безопасности национального информационного пространства, установление норм и механизмов управления своим информационным и культурным пространством в соответствии с национальным законодательством»[16].

Н.П. Ромашкина трактует информационный суверенитет как способность государства обеспечивать независимость и конституционные права граждан в информационном пространстве[17].

Е.С. Зиновьева и С.В. Шитьков рассматривают цифровой суверенитет как динамическую категорию, меняющуюся с развитием государственной политики и технологий (Зиновьева, Шитьков, 2023). В контексте этой дискуссии все большее внимание привлекает проблема соотношения кибербезопасности и суверенитета: новейшие исследования фиксируют нарастающую конкуренцию национальных моделей цифрового суверенитета и связанные с этим вызовы для международного правопорядка (Лазарь, 2025).

Россия выступает за принятие под эгидой ООН конвенции о международной информационной безопасности, которая учитывала бы различные аспекты применения международного права в сфере ИКТ[18]. Для этих целей российские эксперты разработали проект Конвенции ООН «О сотрудничестве в сфере противодействия информационной преступности»[19],

[14] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[15] Ibid.

[16] Ibid.

[17] Ромашкина Н.П. Информационный суверенитет или почему России нужна стратегия информационной безопасности // Российский совет по международным делам. 06.08.2019. URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnyy-suverenitet-ili-pochemu-rossii-nuzhna-strategiya-informatsionnoy-bezopasnosti/ (дата обращения: 28.09.2025).

[18] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[19] Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия

а в 2023 г. предложили на рассмотрение «Концепцию конвенции ООН по международной информационной безопасности»[20].

В российской доктрине необходимость формирования комплексного режима международной информационной безопасности подробно обосновывается в коллективной монографии под ред. А.А. Стрельцова, А.Я. Капустина и др., где анализируются военно-политические, правовые и технологические измерения использования ИКТ в целях стратегического сдерживания и обеспечения безопасности (Международная безопасность…, 2023).

Западные подходы к цифровому суверенитету

Позиции западных государств различаются в деталях, но объединены общим подходом к применению действующего международного права.

США выражают свою позицию следующим образом: во-первых, они подтверждают, что принцип территориальной юрисдикции сохраняет свою значимость даже применительно к кибератакам; во-вторых, подчеркивается, что осуществление юрисдикции государством на своей территории не является абсолютным и должно соответствовать нормам международного права, включая международные обязательства в области прав человека[21]. К. Баннелье-Кристакис предлагает концепцию «киберосмотрительности» (*cyber diligence*) как минимального нормативного стандарта, обязывающего государства предотвращать использование их информационной инфраструктуры для трансграничных кибератак (Bannelier-Christakis, 2014). А. Коко и Т. де Соуза Диас показали, что принцип должной осмотрительности в киберпространстве остается «лоскутным» и фрагментарно закрепленным в различных отраслях международного права, что затрудняет формирование единого режима превентивной ответственности государств (Coco & de Souza Dias, 2021).

Основная проблема заключается в отсутствии четких критериев определения территориальной юрисдикции в киберпространстве. М. Шмитт систематизирует эти «серые зоны» международного права в киберпространстве, показывая, что именно неопределенность порогов суверенитета и юрисдикции позволяет государствам действовать ниже уровня правовой квалификации, избегая ответственности (Schmitt, 2017a). Кибероперации могут проводиться через серверы, расположенные в различных государствах, что затрудняет определение применимого права (Giovanelli, 2025). Требуется разработка международных стандартов разграничения юрисдикций и координации правоприменительной практики.

Со своей стороны МККК запустил проект по разработке цифровой эмблемы, предназначенной для того, чтобы «подсветить» гражданские объекты в сети. В сотрудничестве с Центром кибердоверия, Университетом Джонса Хопкинса и Университетом ИТМО (г. Санкт-Петербург) МККК разработал технические решения для обозначения цифровой инфраструктуры пользующихся защитой организаций в киберпространстве[22].

информационной преступности // Министерство иностранных дел Российской Федерации. 19.01.2018. URL: https://www.mid.ru/ru/foreign_policy/un/1561374/ (дата обращения: 28.09.2025).

[20] Обновленная Концепция конвенции Организации Объединенных Наций об обеспечении международной информационной безопасности // Совет Безопасности Российской Федерации. 16.05.2023. URL: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf (дата обращения: 28.09.2025).

[21] Официальный сборник добровольно представляемых национальных материалов по вопросу о том, как международное право применяется к использованию информационно-коммуникационных технологий государствами. A/76/136 // Организация Объединенных Наций. 13.07.2021. URL: https://documents.un.org/doc/undoc/gen/n21/189/50/pdf/n2118950.pdf (дата обращения: 28.09.2025).

[22] МККК предлагает ввести цифровую эмблему красного креста/красного полумесяца, которая станет знаком защиты в киберпространстве // Международный комитет Красного Креста. 03.11.2022. URL: https://www.icrc.org/ru/document/mkkk-predlagaet-vvesti-cifrovuyu-emblemu-krasnogo-krestakrasnogo-polumesyaca-kotoraya (дата обращения: 28.09.2025).

Кибератаки: определение и атрибуция ответственности

Понятие «кибератака» в международном гуманитарном праве

Исходя из ст. 49 Дополнительного протокола I, в «Таллинское руководстве 1.0» было предложено следующее определение кибератаки: «Кибератака — это кибероперация, будь то наступательная или оборонительная, которая, как обоснованно ожидается, ведет к травмам или смерти людей или повреждению или уничтожению объектов» (Schmitt, 2013, p. 106). То есть только те «военные операции», которые представляют собой «акт насилия», могут называться «нападениями» и, следовательно, должны рассматриваться как запрещенные в соответствии с МГП.

Г.Г. Шинкарецкая обращает внимание, что существующие дефиниции термина «кибератака» не учитывают особенности кибервоздействий, не приводящих к физическому ущербу, и обосновывает необходимость выработки самостоятельного определения кибератаки, отражающего специфику цифровой среды (Шинкарецкая, 2023).

Однако кибероперации обычно не являются «насильственными», что представляет проблему, если пытаться применить к ним нормы МГП. Что касается термина «военные действия», то применительно к кибероперациям его использование может потребовать дополнений к МГП.

Согласно позиции, принятой Международным Комитетом Красного Креста, любая операция в ходе вооруженного конфликта, целью которой является нарушение функционирования компьютера или компьютерной сети, квалифицируется как нападение в соответствии с определением международного гуманитарного права, вне зависимости от способа выведения объекта из строя — будь то физическое уничтожение или иные методы воздействия[23].

По мнению российского специалиста в области права Я.М. Хаминского, среди ключевых вызовов, связанных с киберпространством, выделяется необходимость решения вопроса о том, следует ли отдельные инструменты и способы ведения кибервойны поставить под полный запрет или установить для них регулирование международными соглашениями (Хаминский, 2021).

Многие эксперты полагают, что с учетом новых технологических разработок необходимо расширить понятие «насилие» и помимо «материального ущерба объектам» включить в него и «вывод из строя инфраструктуры без разрушения» (Roscini, 2014, p. 181; Gisel, Rodenhäuser & Dörmann, 2020). Аналогичную позицию занимает Х. Лин, указывающий, что классические категории МГП — «нападение», «средства ведения войны», «военная необходимость» — при буквальном толковании не охватывают значительную часть кибервоздействий, и предлагающий функциональный подход к их квалификации (Lin, 2012).

Р. Бьюкен и Н. Цагуриас дополнительно ставят вопрос об ответственности командования за применение автономных кибер-средств, показывая, что автоматизация атак усложняет не только атрибуцию, но и соблюдение принципов их различения и соразмерности (Buchan & Tsagourias, 2020).

Представляется целесообразным распространить нормы МГП на кибероперации без разрушительных последствий, включая дезактивацию военных систем, вмешательство в информационные сети, разведывательные операции, временный вывод из строя инфраструктуры и психологические операции.

[23] International Humanitarian Law and Cyber Operations during Armed Conflicts // International Committee of the Red Cross. November 28, 2019. URL: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts (accessed: 28.09.2025).

Проблемы атрибуции ответственности в киберпространстве

На настоящий момент атрибуция ответственности представляет собой одну из сложно решаемых задач ввиду возможности использования атакующими государствами территории третьих стран и прокси-игроков. Н. Цагуриас одним из первых показал, что анонимность и трансграничный характер кибератак подрывают традиционные механизмы атрибуции ответственности за эти атаки и ставят под вопрос реализацию права на самооборону, предусмотренного ст. 51 Устава ООН (Tsagourias, 2012).

Сегодня международно-правовая атрибуция носит спекулятивно-субъективный характер и может быть использована для решения собственных политических задач или в качестве инструмента информационной войны для подрыва имиджа стратегического соперника (Ромашкина, Марков, Стефанович, 2020). Единые механизмы раскрытия методологии проведения атрибуции и предоставления исчерпывающей доказательной базы международному сообществу отсутствуют. Н. Цагуриас и М. Фаррелл подчеркивают, что разрыв между техническими и правовыми стандартами атрибуции остается ключевым препятствием для формирования международного режима ответственности за кибероперации (Tsagourias & Farrell, 2020).

По оценкам российских аналитиков, в информационной сфере влияние негосударственных и неправительственных субъектов достигло уровня, сопоставимого с государственной мощью (Коротков, Зиновьева, 2011). Согласно официальной российской позиции, любые обвинения государств в организации и совершении противоправных действий должны иметь под собой веские основания, а публичное возложение ответственности за инциденты в информационном пространстве на конкретное государство недопустимо без предъявления соответствующих технических доказательств[24].

Руководство США, напротив, считает, что не существует международно-правового обязательства раскрывать доказательства, на которых основывается присвоение кибератаки. Поэтому государству не требуется абсолютной уверенности, поскольку оно выступает в качестве своего собственного судьи и может принять одностороннее решение в отношении присвоения кибероперации другому государству[25]. К. Айхензер детально анализирует политико-правовую логику этой позиции, показывая, что атрибуция в практике США выполняет одновременно функцию расширения полномочий исполнительной власти и инструмента сдерживания, при этом стандарт доказательств остается ниже судебного порога (Eichensehr, 2020).

Резолюция 70/237 Генеральной Ассамблеи ООН (ГА ООН) призывает государства к сотрудничеству в обмене информацией и привлечении к ответственности лиц, причастных к преступному использованию ИКТ. 24 декабря 2024 г. на сессии ГА ООН была единогласно поддержана предложенная Россией «Конвенция против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных

[24] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[25] См., например: Eichensehr K. Cyberattack Attribution and International Law // Just Security. July 24, 2020. URL: https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/ (accessed: 05.03.2026). Автор, обобщая практику и заявления США, отмечает, что, несмотря на предложения некоторых государств, не существует международно-правового обязательства раскрывать доказательства, на которых основывается атрибуция кибероперации (“There is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action”).

систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям»[26].

Д.Д. Штодина характеризует принятие данной Конвенции как итог «киберкомпромисса», в котором противоречия между западным и незападным подходами были урегулированы ценой рамочности формулировок, оставляющих значительное пространство для национальной интерпретации (Штодина, 2025).

Тем самым на универсальном уровне закрепляется тенденция к формированию специальных договорных механизмов обмена технической и доказательной информацией о киберинцидентах, что потенциально может способствовать выработке более прозрачных процедур международно-правовой атрибуции и укреплению доверия между государствами в сфере ИКТ.

Разграничение военных и гражданских целей в киберпространстве

Принцип различия между военными и гражданскими целями в киберпространстве осложняется двойным назначением цифровых объектов. Вашингтон в отношении своих подходов к кибероперациям подчеркивает, что даже если нормы права войны формально не применяются, поскольку предполагаемая военная кибероперация осуществляется вне рамок вооруженного конфликта, Министерство обороны все равно руководствуется принципами права войны[27].

«Таллинское руководство 2.0» устанавливает, что гражданские объекты в киберпространстве пользуются защитой от прямых атак (Schmitt, 2017b).

Россия предостерегает от попыток «навязать принцип полной и автоматической применимости международного гуманитарного права к информационно-коммуникационной среде в мирное время»[28]. Российские специалисты отмечают, что гуманитарные объекты критической информационной инфраструктуры не имеют специальных отличительных признаков, подтверждающих их особый правовой статус, и в условиях информационной войны провести четкое разграничение между гражданскими и военными целями крайне затруднительно (Коротков, Зиновьева, 2011; Аду, Рамич, 2025).

Российская позиция состоит в том, что «информационная среда обладает уникальными техническими и правовыми характеристиками, которые не позволяют автоматически и в полном объеме применять к ней действующие нормы международного права. Речь, в частности, о таких особенностях, как трансграничный и всепроникающий характер ИКТ, анонимность их использования и сложность достоверного определения источника вредоносного воздействия, возможность внедрения скрытых вредоносных функций и программно-аппаратных уязвимостей, допустимость применения ИКТ для целей двойного назначения»[29].

---

[26] Конвенция против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям // Организация Объединенных Наций. 24.12.2024. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 28.09.2025).

[27] Ney Jr. P.C. DoD General Counsel Remarks at U.S. Cyber Command Legal Conference // U.S. Department of War. March 2, 2020. URL: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference (accessed: 28.09.2025).

[28] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[29] Выступление представителя Российской Федерации И.А. Тяжловой на седьмой сессии Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 по пункту повестки дня «Как международное право применяется к использованию ИКТ государствами» // Постоянное представительство Российской Федерации при ООН. 06.03.2024. URL: https://russiaun.ru/ru/news/060324 (дата обращения: 29.09.2025).

Таким образом, существующие определения военных и гражданских объектов в МГП нуждаются в уточнении, поскольку военные системы функционируют на базе гражданской инфраструктуры.

Защита критической инфраструктуры

Особую проблему представляет защита критически важной информационной инфраструктуры. Системы энергоснабжения, водоснабжения, транспорта и связи являются преимущественно гражданскими объектами, но могут вносить эффективный вклад в военные действия[30].

Датское[31] и норвежское военные руководства[32] предусматривают возможность атак на объекты двойного назначения при соблюдении принципа соразмерности.

Согласно позиции МККК, особому режиму защиты в рамках международного гуманитарного права подлежат информационные массивы, относящиеся к медицинским учреждениям, гуманитарным организациям и системам жизнеобеспечения гражданского населения, таким как водоочистные сооружения и комплексы ирригации[33]. В рамках разработки «цифровой эмблемы» МККК планирует применять ее и для защиты медицинских объектов в киберпространстве[34].

Защита персональных данных граждан от злоумышленных действий в киберпространстве в условиях вооруженных конфликтов становится все более значимой задачей.

Дискуссионным остается вопрос о статусе данных как объекта защиты по МГП. Большинство экспертов — составителей Таллинское руководства пришли к выводу, что данные *per se* не являются объектами в понимании ст. 52 Дополнительного протокола I (Schmitt, 2017b).

Согласно позиции Министерства обороны Дании, цифровые данные обычно не классифицируются как объект[35].

В противоположность этому военное ведомство Норвегии придерживается мнения, что данные следует относить к категории объектов, а непосредственная атака на них допустима исключительно в случаях, когда они представляют собой легитимную военную цель[36].

По мнению французской стороны, различные виды информационного контента (включая гражданские, банковские и медицинские сведения) находятся под защитой в соответствии с принципом разграничения гражданских и военных объектов[37].

---

[30] Roguski P. France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I // Opinio Juris. September 24, 2019. URL: https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accessed: 28.09.2025).

[31] Military Manual for the Danish Defence // The Danish Armed Forces. October 12, 2020. URL: https://www.forsvaret.dk/en/publications/military-manual/ (accessed: 28.09.2025).

[32] Manual i krigens folkerett. Oslo : Forsvarssjefen, 2013 // Базы данных по международному гуманитарному праву. URL: https://ihl-databases.icrc.org/ru/national-practice/manual-i-krigens-folkerett?activeTab=all-national-practice (accessed: 28.09.2025).

[33] The Use of ICTs in Armed Conflicts Poses a Real Risk of Harm to Civilians and Civilian Infrastructure // International Committee of the Red Cross. July 28, 2022. URL: https://www.icrc.org/en/document/icts-armed-conflicts-risk-harm-civilians-civilian-infrastructure (accessed: 28.09.2025).

[34] Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks and Possible Solutions. International Committee of the Red Cross, 3 November 2022. URL: https://www.icrc.org/en/document/icrc-digital-emblems-report (accessed: 28.09.2025).

[35] Military Manual for the Danish Defence // The Danish Armed Forces. October 12, 2020. URL: https://www.forsvaret.dk/en/publications/military-manual/ (accessed: 28.09.2025).

[36] Manual i krigens folkerett. Oslo : Forsvarssjefen, 2013 // Базы данных по международному гуманитарному праву. URL: https://ihl-databases.icrc.org/ru/national-practice/manual-i-krigens-folkerett?activeTab=all-national-practice (accessed: 28.09.2025).

[37] Roguski P. France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I // Opinio Juris. September 24, 2019. URL: https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accessed: 28.09.2025).

Данный подход критикуется российскими экспертами, указывающими на возможность причинения существенного ущерба гражданскому населению через воздействие на данные без физического повреждения инфраструктуры (Гаркуша-Божко, 2021). Требуется дальнейшая проработка правового статуса данных в контексте защиты гражданских объектов.

Представляется, что в условиях растущей цифровой взаимозависимости общества игнорирование данных как самостоятельного объекта защиты фактически размывает гуманитарные гарантии, заложенные в МГП. Датская позиция, исходящая из того, что цифровые данные «обычно» не рассматриваются в качестве объекта, отражает осторожный, но в долгосрочной перспективе недостаточный подход, поскольку не позволяет адекватно учесть последствия кибероперaций, нацеленных на информационные массивы, от которых зависят жизнь и здоровье гражданского населения. Норвежский и французский подходы, напротив, выглядят более согласующимися с гуманитарной целью МГП, поскольку прямо признают необходимость учитывать воздействие на данные в рамках режима вооруженного конфликта и привязывают допустимость атак к критерию легитимной военной цели и принципу разграничения. В этой связи наиболее обоснованным представляется эволюционное развитие МГП в направлении признания по крайней мере отдельных категорий данных (медицинских, гуманитарных, критически важных для жизнеобеспечения) в качестве объектов, пользующихся особой защитой, с последующей выработкой четких критериев их отнесения к гражданским или военным целям и соответствующей адаптацией правил соразмерности и предосторожности.

Заключение

Проведенный анализ трех ключевых аспектов применения МГП к кибероперациям выявляет существенные пробелы в международном правовом регулировании данной сферы.

Во-первых, в рамках дискуссии вокруг цифрового суверенитета отсутствует международный консенсус относительно объема суверенных прав государств в киберпространстве. Российский подход к информационному суверенитету не получил достаточного отражения в западных концепциях применения МГП. Требуется разработка международных стандартов разграничения юрисдикций и координации правоприменительной практики.

Во-вторых, существующие определения кибератак не учитывают специфику информационно-психологических воздействий. Проблемы атрибуции требуют разработки новых международных механизмов расследования киберинцидентов с едиными стандартами доказательств.

Наконец, принцип различения целей кибератак нуждается в адаптации к условиям цифровой среды. Необходимо уточнение правового статуса данных и критериев защиты объектов двойного назначения.

Перспективы дальнейших исследований в данной сфере связаны с разработкой конкретных механизмов имплементации МГП в киберпространстве и изучением практики государств по реагированию на киберугрозы в контексте международного гуманитарного права. Только синхронизация правовых, технологических и политических аспектов позволит создать устойчивую систему регулирования цифровых конфликтов.

Поступила в редакцию / Received: 20.06.2023
Доработана после рецензирования / Revised: 13.11.2025
Принята к публикации / Accepted: 18.12.2025

Список литературы

Аду Я.Н., Рамич М.С. Разграничение гражданских и военных объектов в условиях развития информационно-коммуникационных технологий в ходе вооруженных конфликтов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2025. Т. 25, № 1. С. 67–77. https://doi.org/10.22363/2313-0660-2025-25-1-67-77; EDN: KACFAB

Гаркуша-Божко С.Ю. Международное гуманитарное право в киберпространстве: Ratione materiae, ratione temporis и проблема квалификации кибератак // Цифровое право. 2021. Т. 2, № 1. С. 64–82. https://doi.org/10.38044/2686-9136-2021-2-1-64-82; EDN: UKFVGJ

Зиновьева Е.С., Шитьков С.В. Цифровой суверенитет в практике международных отношений // Международная жизнь. 2023. № 3. С. 38–51. EDN: HBTQYT

Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО-Университета. 2011. № 4. С. 154–162. EDN: OOQRAD

Лазарь К.К. Кибербезопасность и суверенитет в киберпространстве: вызовы и перспективы международного права // Московский журнал международного права. 2025. № 1. С. 125–137. https://doi.org/10.24833/0869-0049-2025-1-125-137; EDN: HLNRTE

Международная безопасность в среде информационно-коммуникационных технологий / под ред. А.А. Стрельцова, А.Я. Капустина, Т.А. Поляковой, А.С. Маркова, Б.Н. Мирошникова. Москва : НАМИБ, 2023. EDN: FBKNHG

Рахман М.М., Дас Т.К. Противодействие кибератакам: пробелы международного права и перспективы их преодоления // Journal of Digital Technologies and Law. 2024. Vol. 2, no. 4. P. 973–1002. https://doi.org/10.21202/jdtl.2024.46; EDN: NNFTQI

Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии. Москва : ИМЭМО РАН, 2020. https://doi.org/10.20542/978-5-9535-0581-9; EDN: NYGUJH

Хаминский Я.М. Роль международного гуманитарного права в эпоху киберугроз // Advances in Law Studies. 2021. Vol. 9, no. 1. P. 56–60. https://doi.org/10.29039/2409-5087-2021-9-1-56-60; EDN: FEWNTC

Шинкарецкая Г.Г. Международное право и война в киберпространстве // Современное право. 2013. № 8. С. 120–126. EDN: QZLCUF

Шинкарецкая Г.Г. Проблема выработки определения кибератаки // Международное право. 2023. № 2. С. 10–21. https://doi.org/10.25136/2644-5514.2023.2.40051; EDN: NYDJJZ

Штодина Д.Д. Конвенция Организации Объединенных Наций против киберпреступности 2024 года — итог «киберкомпромисса»? // Московский журнал международного права. 2025. № 1. С. 110–124. https://doi.org/10.24833/0869-0049-2025-1-110-124; EDN: XIIYBP

Bannelier-Christakis K. Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations? // Baltic Yearbook of International Law. 2014. Vol. 14, iss. 1. P. 23–39. https://doi.org/10.1163/22115897-90000118

Buchan R., Tsagourias N. Autonomous Cyber Weapons and Command Responsibility // International Law Studies. 2020. Vol. 96. P. 645–673. URL: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2935&context=ils (accessed: 12.02.2025).

Coco A., de Souza Dias T. 'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law // European Journal of International Law. 2021. Vol. 32, iss. 3. P. 771–806. https://doi.org/10.1093/ejil/chab056; EDN: ODWVJK

Droege C. Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians // International Review of the Red Cross. 2012. Vol. 94, iss. 886. P. 533–578. https://doi.org/10.1017/S1816383113000246

Eichensehr K.E. The Law and Politics of Cyberattack Attribution // UCLA Law Review. 2020. Vol. 67, no. 3. P. 520–598. URL: https://www.uclalawreview.org/wp-content/uploads/securepdfs/2020/09/Eichensehr-67-3.pdf (accessed: 12.02.2025).

Giovanelli D. Handling Cyberspace's State of Intermediacy Through Existing International Law // International Review of the Red Cross. 2025. Vol. 107, iss. 928. P. 96–139. https://doi.org/10.1017/S1816383124000390; EDN: GFPZVF

Gisel L., Rodenhäuser T., Dörmann K. Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts // International Review of the Red Cross. 2020. Vol. 102, iss. 913. P. 287–334. https://doi.org/10.1017/S1816383120000387; EDN: ZLBTAJ

Jensen E.T. The Tallinn Manual 2.0: Highlights and Insights // Georgetown International Law Journal. 2017. Vol. 48, iss. 3. P. 735–778. URL: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf (accessed: 13.02.2025).

Lin H. Cyber Conflict and International Humanitarian Law // International Review of the Red Cross. 2012. Vol. 94, iss. 886. P. 515–531. https://doi.org/10.1017/S1816383112000811

Melzer N. Cyberwarfare and International Law. Geneva : UNIDIR, 2011. URL: https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf (accessed: 13.02.2025).

Roscini M. Cyber Operations and the Use of Force in International Law. Oxford : Oxford University Press, 2014. https://doi.org/10.1093/acprof:oso/9780199655014.001.0001

Schmitt M.N. Grey Zones in the International Law of Cyberspace // Yale Journal of International Law Online. 2017a. Vol. 42, no. 2. P. 1–21. URL: https://bpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (accessed: 13.02.2025).

Schmitt M.N., Pakkam A.S. Cyberspace and the *Jus ad Bellum*: The State of Play // International Law Studies. 2024. Vol. 103. P. 194–229. URL: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3085&context=ils (accessed: 18.02.2025).

Schmitt M.N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge : Cambridge University Press, 2017b. https://doi.org/10.1017/9781316822524

Schmitt M.N. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge : Cambridge University Press, 2013. https://doi.org/10.1017/CBO9781139169288

Tsagourias N. Cyber Attacks, Self-Defence and the Problem of Attribution // Journal of Conflict and Security Law. 2012. Vol. 17, iss. 2. P. 229–244. https://doi.org/10.1093/jcsl/krs019

Tsagourias N., Farrell M. Cyber Attribution: Technical and Legal Approaches and Challenges // European Journal of International Law. 2020. Vol. 31, iss. 3. P. 941–967. https://doi.org/10.1093/ejil/chaa057; EDN: JKNLRK

Сведения об авторе:

Козюлин Вадим Борисович — кандидат политических наук, главный научный сотрудник Центра военно-политических исследований, Институт актуальных международных проблем; доцент кафедры государственного управления, Дипломатическая академия МИД России; Российская Федерация, 119021, г. Москва, ул. Остоженка, д. 53/2, строение 1; eLibrary SPIN-код: 6736-6554; ORCID: 0000-0001-6705-5303; e-mail: v.kozyulin@dipacademy.ru