https://doi.org/10.38044/2686-9136-2021-2-1-64-82



СТАТЬИ

# МЕЖДУНАРОДНОЕ ГУМАНИТАРНОЕ ПРАВО В КИБЕРПРОСТРАНСТВЕ: RATIONE MATERIAE, RATIONE TEMPORIS И ПРОБЛЕМА КВАЛИФИКАЦИИ КИБЕРАТАК

**С.Ю. Гаркуша-Божко**

Школа высшего спортивного мастерства
по водным видам спорта имени Ю. С. Тюкалова
197110, Россия, Санкт-Петербург, Набережная Гребного канала, 10, стр. 1

## Аннотация

Целью статьи является анализ таких проблем применения норм международного гуманитарного права (МГП) в киберпространстве, как проблема *ratione materiae* и *ratione temporis* данной отрасли международного публичного права в киберпространстве. Актуальность исследования подтверждается стремительным развитием информационных технологий, которые могут быть использованы в ходе вооруженного конфликта. Факт наличия «Таллиннского руководства 2.0» по международному праву, применимому к кибероперациям, также служит подтверждением актуальности настоящей темы. Использование сторонами вооруженного конфликта в киберпространстве новых технологий никак не влияет на применимость к таким военным действиям норм МГП. Какие именно кибероперации являются предметом регулирования права кибернетических вооруженных конфликтов? Этот вопрос, по нашему мнению, является ключевым. При этом киберпространство представляет собой не совсем обычный театр войны, поскольку средства и методы ведения военных действий никак не связаны с традиционным применением вооруженной силы. В статье уделяется внимание двум основным точкам зрения в отношении этой проблемы. В результате проведенного исследования автор приходит к выводу о том, что при всей очевидности теоретических выводов в отношении анализируемых проблем, они все равно не представляются всеобъемлющими в силу отсутствия соответствующей практики государств, которую необходимо развивать.

## Ключевые слова

международное гуманитарное право, вооруженный конфликт, киберпространство, военные действия, кибероперации, кибератака, нападение, Таллиннское Руководство

| | |
|---|---|
| **Конфликт интересов** | Автор сообщает об отсутствии конфликта интересов. |
| **Финансирование** | Исследование не имело спонсорской поддержки. |

**Для цитирования** Гаркуша-Божко, С. Ю. (2021). Международное гуманитарное право в киберпространстве: Ratione materiae, ratione temporis и проблема квалификации кибератак. *Цифровое право, 2*(1), 64–82. https://doi.org/10.38044/2686-9136-2021-2-1-64-82

Поступила: 23.12.2020; принята в печать: 19.02.2021; опубликована: 31.03.2021

**ARTICLES**

# INTERNATIONAL HUMANITARIAN LAW IN CYBERSPACE: RATIONE MATERIAE, RATIONE TEMPORIS AND THE PROBLEM OF CYBER-ATTACK QUALIFICATION

**Sergey Y. Garkusha-Bozhko**

School of Higher Sportsmanship in Water Sports
named after Y. S. Tyukalov
1-10, Naberezhnaya Grebnogo Canala, St. Petersburg, Russia, 197110

## Abstract

The purpose of the article is to analyse problems arising from applying the rules of International Humanitarian Law in cyberspace, particularly the problems of *ratione materiae* and *ratione temporis* of this branch of Public International Law in cyberspace. The rapid development of cyber technologies that can be used within an armed conflict affirm the applicability of this research. The existence of "The Tallinn Manual 2.0" on International Law Applicable to Cyber Operations also confirms the impact of this topic on the modern world. The fact that parties in armed conflicts use new technologies in cyberspace does not affect the applicability of IHL rules to such military actions. In the context of this issue, a key question which instigates scientific discussion is that of which cyber operations are subject to the regulation of the law of cyber armed conflicts. The urgent need to study this problem stems from the fact that cyberspace is not an ordinary theatre of war, with the means and methods of warfare used in it being in no way related to the traditional use of armed force; given this quality of cyber operations, it is essential to understand which areas may be subject to IHL. The article analyses two main doctrinal points of view in relation to this problem; as this doctrine (in the context of this issue) also addresses the legal qualification of cyber-attacks, the article also raises this topical issue. Based on the results of this analysis, the author concludes that, despite all the evidence of theoretical conclusions regarding the problems under analysis, they still do not seem comprehensive due to the lack of relevant state practice, which needs to be developed.

## Keywords

International Humanitarian Law, armed conflict, cyberspace, hostilities, cyber-operations, cyber-attack, attack, Tallinn Manual

| | |
|---|---|
| **Conflict of interest** | The author declares no conflict of interest. |
| **Financial disclosure** | The study had no sponsorship. |
| **For citation** | Garkusha-Bozhko, S. Y. (2021). International humanitarian law in cyberspace: Ratione materiae, ratione temporis and problem of cyber-attack qualification. *Digital Law Journal, 2*(1), 64–82. https://doi.org/10.38044/2686-9136-2021-2-1-64-82 |

Submitted: 23 Dec. 2020, accepted: 19 Feb. 2021, published: 31 Mar. 2021

## Введение

Развитие информационных технологий в наше время затрагивает все сферы деятельности человечества в мировом масштабе. Не стала исключением и сфера военной деятельности государств. На настоящий момент уровень развития военных информационных технологий позволяет говорить о возможности распространения военных действий на информационное пространство, или как его еще называют киберпространство (англ. *cyberspace*). Иными словами, в современном мире вооруженный конфликт в киберпространстве перестал быть выдумкой писателей-фантастов и сценаристов фантастических развлекательных фильмов — теперь это потенциально возможный конфликт, который может начаться из-за столкновения интересов двух и более государств в киберсфере. Вероятность такого конфликта также подтверждает заявление Президента России В. В. Путина, который отметил, что «одним из основных стратегических вызовов современности является риск возникновения масштабной конфронтации в цифровой сфере»[1].

Как отмечают в доктрине (Melzer, 2017), киберпространство является «пятой сферой или пятым доменом ведения военных действий» после суши, моря, воздушного и космического пространств. Данное утверждение не может быть оспорено по той причине, что в силу уровня развития современных технологий киберпространство, в действительности, является потенциальным театром военных действий. Высокая вероятность таких вооруженных конфликтов заставила государства задуматься об их правовом регулировании, и в 2013 году благодаря усилиям юристов и военных специалистов из стран военно-политического блока НАТО, при участии специалистов из Международного Комитета Красного Креста (МККК), было разработано «Таллиннское руководство по международному праву, применимому к кибервооружениям» (англ. "*Tallinn Manual on the International Law Applicable to Cyber Warfare*") (далее — Руководство) (Schmitt, 2013).

Руководство является попыткой разработать нормы международного права, применимые не только к такому роду вооруженных конфликтов, но и к киберпространству в целом, как в военное, так и в мирное время. Необходимость международно-правовых норм в этой области очень высока, что и обусловило принятие новой расширенной версии Руководства в 2017 г. Его существование лишний раз доказывает актуальность как проблемы правового регулирования вооруженных конфликтов в киберпространстве, так и проблемы правового регулирования киберпространства в целом.

[1] Путин, В. В. (2020, сентябрь 25). *Заявление о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности*. Официальный сайт Президента РФ. http://kremlin.ru/events/president/news/64086

Факт использования сторонами вооруженного конфликта в ходе военных действий в киберпространстве новых технологий никак не влияет на применимость к таким действиям норм международного гуманитарного права (МГП). Тем не менее, в силу различных особенностей киберпространства, в частности, анонимности его пользователей, при применении к кибернетическим военным действиям норм МГП возникает ряд проблем. Одной из которых, является вопрос о том, какие именно кибероперации становятся предметом регулирования права кибернетических вооруженных конфликтов? Иными словами, речь идет о *ratione materiae* МГП в киберпространстве. Эта проблема является предметом активных научных дебатов (Droege, 2012; Backstrom & Henderson, 2012; Schmitt, 2017; Zhang, 2012; Schmitt, 2002).

Ключевым моментом для применения норм международного гуманитарного права к киберпространству считается наличие фактической ситуации вооруженного конфликта в киберпространстве. Однако важно понимать, какие именно кибероперации будут регулироваться такими нормами, поскольку понимание обеспечивает соблюдение норм МГП в киберпространстве.

Причины необходимости исследования вопроса *ratione materiae* международного гуманитарного права в киберпространстве достаточно просты: киберпространство представляет собой не совсем обычный театр войны, т. к. средства и методы ведения военных действий, применяемых в нем, никак не связаны с традиционным применением вооруженной силы. Большинство кибероперaций направлено на длительное воздействие на объект кибернетического нападения с целью нарушения его нормального функционирования, но последствия такого негативного воздействия редко приводят к физическому разрушению или повреждению, что происходит в ходе традиционного вооруженного конфликта. Исходя из такой природы кибероперaций, крайне важно понять, какие из них могут являться предметом МГП. Особенно важно это понять в отношении кибероперaций, которые могут затронуть лиц, находящихся под защитой норм «права Женевы» — в первую очередь, это касается вопросов защиты гражданского населения. В современных условиях большинство информационных систем все-таки имеет гражданский характер, поэтому достаточно легко представить сценарии кибернетического вооруженного конфликта, в которых будет затронуто гражданское население.

Привести примеры ситуаций, в которых кибероперации будут затрагивать гражданское население, достаточно легко; причем они вызывают вопросы правовой квалификации, как в военное время, так и в мирное. К примеру, осуществление кибероперации, направленной на нарушение функционирования гражданской энергетической системы или системы водоснабжения без их физического разрушения.

Также можно привести пример компьютерного вируса *Stuxnet*, который имел своей целью нарушение нормального функционирования завода по обогащению урана в Исламской Республике Иран, в городе Нетензе. Настоящий пример является одним из ярчайших примеров длительного враждебного воздействия на соответствующие государственные информационные системы. Как было установлено, данный вирус был разработан при участии экспертов из спецслужб США и Израиля, и его целью была ядерная программа Ирана[2].

Государства, в частности, Иран, не квалифицировали ситуацию с вирусом *Stuxnet* в качестве нападения. Несмотря на это обстоятельство в доктрине была высказана мысль, согласно которой международный вооруженный конфликт в киберпространстве возникает, когда возможно установить конкретное государство, разработавшее вирус (Schmitt, 2012; Brown, 2011).

[2] Nakashima, E., & Warrick, J. (2012, June 1). *Stuxnet was work of U.S. and Israeli experts, officials say*. The Washington Post. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Так, G. D. Brown (2011) прямо заявляет, что вирус *Stuxnet* является кибератакой, возможно, в нарушение основополагающего международно-правового принципа неприменения силы и угрозы ею, а также в нарушение норм *jus in bello*. Исходя из таких заявлений в доктрине, вполне может возникнуть мысль о возможных кибератаках, осуществляемых неправительственной группой против правительства того или иного государства, что повлечет за собой вопрос о квалификации такого случая в качестве немеждународного вооруженного конфликта в киберпространстве.

Приведем другой пример ситуации, в отношении которой также звучали призывы к квалификации совершенных кибератак в качестве актов «кибервойны». Речь идет о кибератаках, совершенных против правительственных и банковских инфраструктур в Эстонии в 2007 году, в результате которых, в том числе, гражданские лица — клиенты пострадавших эстонских банков лишились доступа к банковским услугам (Tikk et al., 2010; Buchan, 2012; Pool, 2013)[3]. Многие журналисты, а также некоторые юристы из западных стран, основываясь на том, что данные кибератаки были совершены после принятия решения о переносе Бронзового солдата, необоснованно обвинили в этих кибератаках Российскую Федерацию (Tikk et al., 2010; Buchan, 2012; Pool, 2013)[4], хотя эксперты доказали непричастность Российской Федерации к этим кибератакам[5]. Мы не будем углубляться в эти споры, которые являются больше политическими, чем юридическими. Отметим только, что данный пример очень хорошо иллюстрирует необходимость определения *ratione materiae* международного гуманитарного права в киберпространстве.

Исходя из вышеперечисленного, мы поставим следующие вопросы. Во-первых, применяются ли нормы международного гуманитарного права только к кибероперациям, которые можно признать нападением, или ко всем военным кибероперациям, и с какого момента такие нормы будут применяться к таким операциям? В этой связи надлежит рассмотреть не только критерий *ratione materiae*, но и *ratione temporis*. Во-вторых, необходимо понять, что такое нападение (кибератака) в киберпространстве? Но перед исследованием вышеуказанных вопросов важно также ответить на вопрос, что такое киберпространство, с чего и начнется настоящее исследование.

## Понятие киберпространства

Несмотря на стремительное развитие информационных технологий, на международном уровне до сих пор нет универсального определения киберпространства, а существует множество определений, закрепленных в различных международных документах.

Так, в статье 2 концепции Конвенции об обеспечении международной информационной безопасности, вынесенной Российской Федерацией в 2011 г. на рассмотрение в Организацию Объединенных Наций (ООН), под информационным пространством понимается сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием,

[3] См. также: Санжиев, А. (2007, июнь 7). *Таллин пошел по миру*. Российская газета. https://rg.ru/2007/06/07/estoniya.html; Орлов, А. (2007, июнь 6). *Атака хакеров на Эстонию шла не из России, а со всего мира — эксперт*. РИА Новости. https://ria.ru/20070606/66760771.html; Vitkine, B. (2017, Mars 14). L'Estonie, première cybervictime de Moscou [Estonia, Moscow's first cybervictime]. Le Monde. https://www.lemonde.fr/international/article/2017/03/14/l-estonie-premiere-cybervictime-de-moscou_5093948_3210.html

[4] Vitkine, 2017.

[5] Санжиев, 2007; Орлов, 2007.

хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию[6].

Аналогичное определение также закреплено в Соглашении между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности[7], в Соглашении между Правительством Российской Федерации и Правительством Республики Беларусь[8] и в Соглашении между Правительством Российской Федерации и Правительством Китайской Народной Республики[9].

В Руководстве под киберпространством понимается среда, образованная физическими и нефизическими компонентами для хранения, модификации и обмена данными с использованием компьютерных сетей (Schmitt, 2013).

Также заслуживает внимания определение, разработанное совместной группой российских и американских специалистов. Они отметили, что под киберпространством понимается электронная среда, в которой информация создаётся, передаётся, принимается, хранится, обрабатывается и уничтожается[10]. Данное определение, по сути, отражает саму суть киберпространства, но оно не учитывает одного важного момента. Речь идет о глобальном характере киберпространства, который обеспечивает возможность информационного обмена и взаимодействия, несмотря на государственные границы. Вместе с тем со стороны большинства государств наметилась тенденция установления суверенитета над своими национальными сегментами глобального киберпространства. Так называемый Закон о «суверенном Интернете»[11], принятый в России в 2019 г., иллюстрирует это.

Однако не следует отождествлять Интернет и киберпространство. Киберпространство включает в себя глобальную сеть Интернет, но не ограничивается ею. В подтверждение этого тезиса можно привести определение киберпространства, закрепленное в Доктрине информационной безопасности Российской Федерации, в которой данное понятие именуется информационной сферой. Здесь под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных

6 МИД России. (2011, сентябрь 22). *Конвенция об обеспечении международной информационной безопасности (концепция)*. https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

7 Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. Бюллетень международных договоров, Март 1993–2012, № 1, с. 13–21.

8 Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 г. Бюллетень международных договоров, Март 1993–2015, № 7, с. 16–23.

9 Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. Бюллетень международных договоров, Март 1993–2016, № 11, с. 82–88.

10 Issuu. (2011, April 26). *The Russia — U. S. bilateral on cybersecurity: Critical terminology foundations*. https://issuu.com/ewipublications/docs/russia-us-terminology

11 Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации». Собрание законодательства Российской Федерации 2019, № 18, Статья 2214.

отношений[12]. Как видно из определения, Интернет не тождественен киберпространству. В доктрине также возможно найти подтверждение тезису о том, что не следует отождествлять Интернет и киберпространство (Danel'yan, 2020). Получается, киберпространство представляет собой совокупность компьютерных сетей, мобильных устройств и пользователей, которые взаимодействуют между собой на расстоянии, а Интернет является связующим каналом для такого взаимодействия.

С учетом вышеуказанного, считаем, что под киберпространством необходимо понимать глобальную электронную среду, образованную физическими и нефизическими компонентами, включая комплекс технических и программных средств, в которой посредством использования компьютерных и мобильных сетей, включая глобальную информационно-коммуникационную сеть «Интернет», осуществляется формирование, передача, прием, хранение, обработка, модификация и уничтожение информации.

## Понятие вооруженного конфликта в киберпространстве

В Руководстве отдельной нормы-дефиниции вооруженного конфликта в киберпространстве не содержится, тем не менее такое определение содержится в пункте 2 комментария к норме 80. Под вооруженным конфликтом понимается ситуация, связанная с осуществлением военных действий, включая те, которые осуществляются с использованием киберсредств. Далее по тексту комментария, разработчики указали, что понятие «вооруженный конфликт» приобретает различное значение в зависимости от его типологии, закрепленной в нормах 82 и 83 Руководства (Schmitt, 2013).

В норме 82 закреплено следующее: «Международный вооруженный конфликт имеет место всякий раз, когда между двумя или более государствами происходят военные действия, которые могут включать кибероперации или ограничиваться ими». В свою очередь, в норме 83 указано, что «немеждународный вооруженный конфликт возникает всякий раз, когда имеет место продолжительное вооруженное насилие, которое может включать или ограничиваться кибероперациями, происходящими между правительственными вооруженными силами и организованными вооруженными группами или между такими группами. Конфронтация должна достигать минимального уровня интенсивности, а вовлеченные в конфликт стороны должны обладать минимальной степенью организованности».

Как представляется, определение, закрепленное в комментарии к норме 80 Руководства, основано на нормах международного гуманитарного права и отражает суть вооруженного конфликта, но в то же время является достаточно общим. Ключевым моментом здесь является то, что такой конфликт осуществляется с использованием киберсредств, под которыми понимаются различные инструменты и методы, используемые в киберпространстве. На это указывают и в доктрине (Lin, 2012). Изучим их более подробно.

Для начала отметим, что предлагается две классификации таких инструментов и методов (Lin, 2012): во-первых, киберсредства можно разделить на автономные, способные работать без вмешательства человека, и на управляемые, которые работают под управлением оператора. Во-вторых, кибер-средства можно разделить на наступательные и оборонительные.

Очевидно, что первая классификация основана на техническом аспекте — в информационных технологиях, как известно, существуют автономные системы,

[12] Доктрина информационной безопасности Российской Федерации. Утв. Указом Президента РФ от 5 декабря 2016 г. № 646. Собрание законодательства Российской Федерации 2016, № 50, Статья 7074.

которые работают без вмешательства человека, а также системы, управляемые оператором. В качестве критерия, лежащего в основе второй классификации, выступает военная тактика.

Предложенные классификации являются пересекающимися: автономные киберсредства могут быть как оборонительными, так и наступательными. Аналогично обстоит дело и с управляемыми киберсредствами. Рассмотрим автономные и управляемые средства, поскольку технический аспект является первичным.

Автономное наступательное киберсредство включает 3 необходимых элемента. Во-первых, доступ, под которым понимаются инструменты и методы, с помощью которых стороны конфликта получают информацию. Важно отметить, что в рамках киберпространства распространен удаленный доступ, который не требует близкого контакта между сторонами, что значительно отличает традиционный вооруженный конфликт от кибернетического.

Во-вторых, различные технические уязвимости той или иной информационной системы, которые позволяют ее взломать и получить доступ к интересующей информации. Сделать киберсистему полностью неуязвимой невозможно. Однако техническая уязвимость может быть оставлена в информационной системе намеренно и представлять собой «ловушку» для другой стороны кибернетического вооруженного конфликта.

И, наконец, в-третьих, так называемая полезная нагрузка, под которой понимается механизм воздействия на информационную систему после проникновения в нее в результате использования ее технической уязвимости. В качестве иллюстрации этого технического термина можно отметить, что, например, в случае компьютерного вируса полезной нагрузкой являются вредоносные действия такого программного обеспечения, которое и является примером автономного наступательного киберсредства. Компьютерные вирусы, как известно, действуют самостоятельно, и вполне возможно, что в ходе вооруженного конфликта в киберпространстве одна из воюющих сторон может использовать программное обеспечение, которое, взломав информационную систему противника, будет собирать необходимую информацию о противнике.

Что же касается автономных оборонительных киберсредств, то принцип их работы основан на использовании одного или нескольких вышеуказанных компонентов. Так, например, работа брандмауэра (файрвола) основана на принципе противодействия несанкционированному доступу в информационную систему, основанному на использовании технических уязвимостей системы.

Что же касается управляемых киберсредств, то тут все проще. Так как управляет таким инструментом оператор, т. е. человек, то объектом первичного воздействия будет именно он. Здесь применяются все те же традиционные наступательные методы по подкупу, вербовке и т. п. Оборонительными методами в таком случае будут различные мероприятия по предотвращению таких действий в отношении оператора.

Важно отметить, что данный подход не оспаривается в доктрине (Lin, 2012). В доктрине некоторые исследователи используют в отношении киберсредств термин «кибероружие» или «информационное оружие» (Talimonchik, 2015; Franklin, 2016; Hathaway et al., 2012; Pool, 2013). В то же самое время понятие «кибероружие» является более узким, поэтому более целесообразно использовать понятие «киберсредства».

Какие действия в киберпространстве могут осуществляться с использованием таких средств? Какие кибероперации существуют?

Так, большинство авторов классифицируют кибероперации на кибератаки и киберэксплуатацию (Lin, 2012; Schmitt, 2013).

В соответствии с нормой 92 Руководства, кибератака — это наступательная или оборонительная кибероперация, которая, как разумно ожидается, приведет к причинению травм или смерти людей, либо к повреждению или разрушению объектов (Schmitt, 2013).

Определение кибератаки также содержится и в национально-правовых актах, например в ст. 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. № 187-ФЗ: «компьютерная атака — целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации»[13].

Данное определение, закрепленное в российском законе, является общим, и не учитывает специфику кибератак в условиях кибернетического вооруженного конфликта. Поэтому более целесообразным будет использование терминологии Руководства.

Киберэксплуатация, в свою очередь, — это кибероперации, направленные на проникновение в информационные системы противника с целью получения интересующей информации и не нарушающие их целостности и нормального функционирования. Как разумно отмечают в доктрине, лучшая киберэксплуатация — это та, которая незаметна для пользователей информационной системы, в которую осуществляется проникновение (Lin, 2012). Поэтому одним из примеров такой кибероперации является кибершпионаж. При этом в прессе порой отдельные кибероперации называют кибератаками, несмотря на то что такие кибероперации являются киберэксплуатацией.

Важно учитывать, что понятие «вооруженный конфликт» приобретает различное значение в зависимости от его типологии. Безусловно, международный вооруженный конфликт отличается от немеждународного в части их правового регулирования — это бесспорный факт. Тем не менее международный и немеждународный вооруженный конфликт являются частными случаями более общего понятия «вооруженный конфликт».

Итак, вооруженный конфликт в киберпространстве — это ситуация вооруженного столкновения и противостояния правительственных вооруженных сил двух и более государств, а также ситуация продолжительного вооруженного противостояния между правительственными вооруженными силами и организованными вооруженными группами или же между такими группами внутри одного государства, уровень напряженности насилия в которой превышает уровень напряженности в ситуациях нарушения внутреннего порядка и возникновения обстановки внутренней напряженности, в контексте которой сторонами такого противостояния используются киберсредства с целью осуществления различных кибероперациий в отношении друг против друга.

Отметим, что целесообразнее использовать понятие «кибернетический вооруженный конфликт», а не «кибервойна». Как известно, при разработке в далеком 1949 г. был использован термин «вооруженный конфликт», а не «война», т. к. первое понятие более широкое, чем второе. Надо полагать, что данная логика применима и к киберпространству. Несмотря на логичность такой аналогии, многие исследователи используют термин «кибервойна» (Zhang, 2012; Droege, 2012; Schmitt, 2002; Pool, 2013).

Теперь, определившись с основными понятиями, перейдем к предмету настоящей статьи.

[13] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» Собрание законодательства Российской Федерации 2017, № 31, Статья 4736.

## *Ratione materiae* МГП в киберпространстве

Для начала определимся с общим понятием военные действия или военные операции. Отправной точкой для этого является ст. 48 Дополнительного Протокола I, которая закрепила обычно-правовую норму, применяемую как в международных, так и немеждународных вооруженных конфликтах (Henckaerts & Doswald-Beck, 2006). В статье закреплено следующее: «Для обеспечения уважения и защиты гражданского населения и гражданских объектов стороны, находящейся в конфликте, должны всегда проводить различие между гражданским населением и комбатантами, а также между гражданскими объектами и военными объектами и соответственно направлять свои действия только против военных объектов»[14].

Определяющим для военных действий (операций) является критерий направленности: они могут быть направленны только против военных целей, т. е. против комбатантов и военных объектов. Такой характер военных операций, в том числе и нападений, предопределен таким принципом международного гуманитарного права, как принцип проведения различия, который пронизывает все нормы, касающиеся вопросов ведения военных действий, как общего, так и конкретного характера. Так, в п. 1 ст. 51 Дополнительного Протокола I указано, что «гражданское население и отдельные гражданские лица пользуются общей защитой от опасностей, возникающих в связи с военными операциями»[15]. Пункт 2 данной статьи указывает, что «гражданское население как таковое, а также отдельные гражданские лица не должны являться объектом нападений»[16]; а в п. 3 закреплен запрет нападений неизбирательного характера[17].

В пп. «b» п. 5 ст. 51 Дополнительного Протокола I нашел отражение не только принцип проведения различия, но и принцип соразмерности: «В числе прочих следующие виды нападений следует считать неизбирательными: ...b) нападение, которое, как можно ожидать, попутно повлечет за собой потери жизни среди гражданского населения, ранения гражданских лиц и ущерб гражданским объектам, или то и другое вместе, которые были бы чрезмерны по отношению к конкретному и непосредственному военному преимуществу, которое предполагается таким образом получить»[18]. Этот принцип тесно связан с принципом проведения различия и, по сути, вытекает из него, на что указывают в доктрине (David, 2011).

Продолжая рассуждения о принципе проведения различия, отметим, что п. 6 ст. 51 Дополнительного Протокола I закрепил запрет нападений на гражданское население (отдельных гражданских лиц) в порядке репрессалий[19], а п. 2 ст. 52 закрепил, что нападения должны строго ограничиваться военными объектами[20].

И, наконец, п. 1 ст. 57 Дополнительного Протокола I закрепил вытекающий из принципа проведения различия принцип предосторожности: «При проведении военных операций постоянно проявляется забота о том, чтобы щадить гражданское население, гражданских лиц и гражданские объекты»[21].

---

[14] Дополнительный протокол (Протокол I) к Женевским конвенциям касающийся защиты жертв международных вооруженных конфликтов ст. 48, Август, 12, 1949, с. 264. [далее — Женевский протокол (I)].

[15] Женевский протокол (I), 265.

[16] Женевский протокол (I), 265.

[17] Женевский протокол (I), 265.

[18] Женевский протокол (I), 265.

[19] Женевский протокол (I), 266.

[20] Женевский протокол (I), 266.

[21] Женевский протокол (I), 269.

Отметим также, что еще одним ограничивающим военные действия фактором является принцип гуманности, который аналогично является одним из ключевых принципов международного гуманитарного права, что прослеживается в нормах этой отрасли международного права, включая выше проанализированные нормы.

Таким образом, все военные действия ограничены вышеуказанными принципами гуманности, проведения различия, соразмерности и предосторожности. Установив этот очевидный факт, перейдем теперь к поставленному выше вопросу в отношении кибероперациий.

В отношении данного вопроса в доктрине существует 3 точки зрения. Первая является наиболее поддерживаемой: большинство исследователей придерживаются мнения, что несмотря на то, что содержание норм Дополнительного Протокола I, в частности его ст. 48 и следующих за ней статей, свидетельствуют о верховенстве в международном гуманитарном праве принципа защиты гражданского населения, только те кибероперации, которые являются нападением (кибератаками), попадают под действие вышеуказанных принципов МГП, в частности, под действие принципа проведения различия (Schmitt, 2011; Geiß & Lahmann, 2012). Так, M. N. Schmitt (2011) выдвигает аргумент, согласно которому определенные военные операции могут быть специально направлены против гражданского населения, в частности, психологические операции, следовательно, не все военные действия в киберпространстве будут ограничиваться принципом проведения различия.

Другая позиция была высказана N. Melzer (2011): научные споры в отношении понятия «нападение» не дают достаточно удовлетворительного ответа на данный вопрос, поскольку нормы права, регулирующие ведение военных действий, применяются ко всем военным операциям, а не только к нападениям. В частности, ученый указывает, что применение закрепленных нормами международного гуманитарного права по отношению к военным операциям ограничений к кибероперациям зависит не от квалификации такой кибероперации в качестве нападения, а от того, является ли такая кибероперация частью военных действий, как это подразумевается в МГП. Исходя из этого, он приходит к выводу о том, что кибероперации должны признаваться военными действиями в случаях, если они направлены на причинение ущерба противной стороне, на причинение смерти или увечий людям, а также на разрушение и повреждение различных объектов, либо в ситуациях, когда они имеют своей целью негативное влияние на военный потенциал противника. Следовательно, в качестве примера кибероперациий, являющихся военными действиями, можно привести такие операции, которые направлены на нарушение функционирования информационных инфраструктур и сетей, с помощью которых противник управляет системам различных вооружений, при этом не требуется, чтобы таким сетям и инфраструктурам был причинен физический вред.

Если взять за основу подход N. Melzer (2011), то из-под понятия «военные действия» выпадают кибероперации, направленные на сбор разведывательных данных. Как известно, разведка также является формой военных действий, поэтому данный подход не отражает ту концепцию военных действий, которая отражена в нормах права вооруженных конфликтов.

Что касается утверждения о том, что не требуется причинения физического ущерба, то N. Melzer (2011) все-таки не делает конкретного вывода, ограничиваясь указанием на проблему нахождения баланса между ограничительным и разрешительным толкованием права.

Принимая во внимание цели норм МГП, в соответствии с которыми «мирное гражданское население должно оставаться за пределами военных действий, насколько это возможно,

и пользоваться общей защитой от опасности, вытекающей из военных действий» (Sandoz et al., 1987), позицию N. Melzer (2011) можно охарактеризовать как верную. Тем не менее в таком случае останется открытым вопрос о том, являются ли операции, направленные на нарушение функционирования гражданской инфраструктуры, военными действиями.

Третья точка зрения была высказана H. H. Dinniss (2012), согласно которой запрет нападений на гражданское население и гражданские объекты распространяется не только на нападения, как таковые. Основываясь на содержании ст. 48, 51 и 57 Дополнительного Протокола I, ученый указывает, что гражданские лица пользуются защитой от военных операций в целом, включая нападения; и поэтому принципы МГП полностью применимы к кибероперациям, в том числе и к кибератакам, которые являются военными действиями, при этом кибератаки должны соотноситься с применением традиционной вооруженной силы, но необязательно должно приводить к таким же последствиям.

Критикуя позицию H. H. Dinniss (2011), C. Droege (2012) отмечает, что в нормах МГП содержится дихотомия между военными операциями и нападениями, чего не учитывает подход Г.Г. Харрисон.

Указанная дихотомия ни в коем случае не влияет на применение к нападениям принципов МГП — ведь определение нападения закрепили лишь потому, что оно является одной из основных военных операций, т. е. является частным явлением общего понятия «военные операции». Кроме того, позиция H. H. Dinniss (2012) лишний раз подтверждает факт, что принципы МГП применяются ко всему комплексу военных действий.

Вернемся к первой точке зрения, выдвинутой M. N. Schmitt (2011), согласно которой психологические операции входят в понятие «военные действия». Отметим, что в доктрине обосновано звучат голоса, что эта позиция основана на неверном толковании концепции военных действий (Droege, 2012). Напомним, что, как справедливо указывают в доктрине (David, 2011), моральный дух врага не является военной целью. Следовательно, действия, направленные на подрыв морального духа врага, в том числе, направленные против его гражданского населения, никак не могут являться военными операциями.

Видимо, M. N. Schmitt (2011) основывал свои рассуждения на тезисе У. Черчилля о том, что «моральный дух неприятеля — тоже военный объект». Мы же обратимся к юридической стороне вопроса о понятии военных операций. Как отмечают в Комментарии к ст. 48 Дополнительного Протокола I, понятие «военные действия» относится ко «всем передвижениям и актам, связанным с военными действиями, которые осуществляются вооруженными силами» (Sandoz et al., 1987). В комментарии к ст. 51 под военными операциями понимаются «все передвижения и деятельность, осуществляемые вооруженными силами в связи с военными действиями» (Sandoz et al., 1987). И, наконец, в комментарии к ст. 57 под военными действиями понимаются «любые передвижения, маневры и любая другая деятельность, осуществляемые вооруженными силами в отношении боевой цели» (Sandoz et al., 1987).

Таким образом, психологические операции, пропаганда, а также шпионаж не относятся к понятию «военные действия». Также отметим, что целью принципов МГП является ограничение всего спектра военных операций, включая нападения. Поэтому надо полагать, что применительно к киберпространству под ограничения, налагаемые МГП, попадают все кибероперации, которые могут быть приравнены к военным действиям в целом, а не только к кибератакам. Это и есть *ratione materiae* международного гуманитарного права в киберпространстве. Аналогичной точки зрения придерживаются и разработчики Руководства.

## *Ratione temporis* МГП в киберпространстве

Исходя из общей ст. 2 Женевских конвенций[22], нормы МГП к киберпространству применяются либо с момента начала вооруженного конфликта, в котором совершаются кибероперации, либо с момента начала вооруженного конфликта, ограниченного киберпространством, без применения традиционной вооруженной силы. Эта составляющая вопроса о *ratione temporis* не вызывает каких-либо трудностей. Сложности возникают при ответе на вопрос об окончании применения таких норм к киберпространству.

Как установлено ст. 6 Женевской конвенции IV[23] и п. «b» ст. 3 Дополнительного Протокола I[24], нормы права вооруженных конфликтов прекращают свое действие по окончанию военных действий. В Комментарии МККК указано, что под окончанием военных действий понимается, в том числе, «последний залп» (Pictet, 1958), заключение перемирия, капитуляция и т. п. (Pictet, 1958; Sandoz et al., 1987). Применительно к киберпространству, моментом окончания следует считать момент завершения последней кибероперации, совершенной в контексте классического или кибернетического вооруженного конфликта. Однако данный вывод все-таки является исключительно теоретическим, поскольку отсутствует соответствующая практика государств.

Вопросы также возникают в отношении окончания оккупации, плена и интернирования. Уже упомянутый пункт «b» ст. 3 Дополнительного Протокола I устанавливает, что МГП прекращает применяться в момент окончания оккупации[25]; ст. 5 Женевской Конвенции III связывает окончание применения норм МГП с моментом окончания плена (полное освобождение военнопленных и их репатриация)[26], а ст. 6 Женевской конвенции IV указывает в этом плане на момент окончания интернирования[27]. Надо полагать, что ко всем кибероперациям, совершенным до обозначенных моментов, будут применяться нормы МГП. Тем не менее данный вывод снова остается исключительно теоретическим.

## Проблема квалификации кибератаки в рамках вооруженного конфликта

Кибератаки отличаются от традиционных нападений тем, что не предполагают классического применения вооруженной силы (применение насилия). П. 1 ст. 49 Дополнительного Протокола I устанавливает, что под нападениями понимаются акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне[28]. Выходит, применение насилия не указывает на средства нападения. Под средствами нападений принято понимать средства, имеющие кинетический эффект (Dinstein, 2016; Schmitt, 2011; Franklin, 2018). Военные действия, в ходе которых применяется оружие, приводящие к серьезным разрушениям и повреждениям объектов и к причинению смерти и увечий, являются нападениями, даже в случае, если отсутствует применение физической силы. Такой вывод

[22] Женевский протокол (I), 240.

[23] Женевская конвенция о защите гражданского населения во время войны, ст. 6, Август, 12, 1949, с. 171. [далее — Четвертая женевская конвенция].

[24] Женевский протокол (I), 241.

[25] Женевский протокол (I), 241.

[26] Дополнительный протокол (Протокол III) к Женевским конвенциям касающийся принятия дополнительной отличительной эмблемы ст. 5, Август, 12, 1949, с. 241. [далее — Женевский протокол (III)].

[27] Четвертая женевская конвенция, 84.

[28] Женевский протокол (I), 264.

подтверждается практикой[29]. Поэтому достаточно долгое время считалось, что определяющим фактором для квалификации военной операции в качестве нападения является не насильственный характер используемых в ее ходе средств, а серьёзность последствий такой операции (Schmitt, 2002; Schmitt, 2013). Признать кибератаки нападениями по смыслу МГП достаточно сложно.

В этом контексте научные споры идут в отношении кибератак, которые не приводят к разрушениям и повреждениям объектов, к смертям и ранениям людей, но приводят к нарушению нормального функционирования атакуемых объектов без какого-либо физического повреждения или разрушения. Негативное влияние таких кибератак в физическом пространстве может быть минимальным с точки зрения того уровня насилия, которое требуется для квалификации деяния в качестве нападения: например, будет прекращена подача электроэнергии или подача питьевой воды, либо будет нарушена система банковских онлайн-платежей и т. п. Возникает закономерный вопрос: могут ли такие кибератаки квалифицироваться в качестве нападения по смыслу ст. 49 Дополнительного Протокола I?

В доктрине можно выделить две основных точки зрения на эту проблему. Первая была выдвинута M. N. Schmitt (2002; 2011). Однако следует учитывать, что его позиция претерпела некоторую эволюцию. В ранних работах ученый отмечал, что кибератака является нападением в соответствии со ст. 49 Дополнительного Протокола I, если она причиняет смерть или увечья людям, вне зависимости от того, являются ли они комбатантами или гражданскими лицами, либо приводит к повреждениям или разрушению объектов как военных, так и гражданских. Таким образом, для признания кибератаки нападением необходимо наличие указанных серьезных последствий в физическом мире. Что касается кибератак, которые причиняют лишь временные неудобства или нарушают нормальное функционирование атакуемой информационной системы, нападением по смыслу ст. 49 Дополнительного Протокола I они не являются.

Несколько позже указанный автор изменил свой подход. И теперь под уничтожением, к которому должна приводить кибератака для того, чтобы ее можно было квалифицировать в качестве нападения, также понимает последствия, которые хоть и не причиняют физического уничтожения (повреждения), но «ломают» информационную систему, выводят ее из строя, что делает невозможным нормальное ее функционирование (Schmitt, 2012a; Schmitt, 2012b; Schmitt, 2014; Schmitt, 2019).

Альтернативная точка зрения была выдвинута К. Дёрманом. Так, по мнению ученого, кибератаки могут являться нападением, даже если отсутствуют традиционные последствия нападений в физическом мире[30]. Такой подход, по сути, основан на п. 2 ст. 52 Дополнительного Протокола I, согласно которому одним из способов воздействия на военные объекты, наряду с разрушением (полное и частичное) и захватом, является нейтрализация[31]. Как отмечает К. Дёрман, нейтрализация вовсе не означает был ли выведен атакуемый военный объект из строя посредством разрушения, уничтожения или посредством любого другого способа[32].

Его оппонент, М.Н. Шмитт, поначалу выразил несогласие с предложенной теорией нейтрализации, указав, что ст. 52 Дополнительного Протокола I, определяющая военные объекты,

---

29 Prosecutor v. Tadić, Case No. IT-94-1-T, decision on the defence motion for interlocutory appeal on jurisdiction. 120, 124 (Int'l Crim. Trib. For the Former Yugoslavia Oct. 2, 1995).

30 Dörmann, K. (2004). *Applicability of the additional protocols to computer network attacks*. ICRC. https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf

31 Женевский протокол (I), 54.

32 Dörmann, 2004.

не имеет отношения к делу, поскольку сама сущность военного объекта предполагает нападение, но не определяет его (Schmitt, 2011). Тем не менее после эволюции его взглядов он принял теорию, предложенную К. Дёрманом, (Schmitt, 2014).

Понять первичную критику позиции K. Dörmann со стороны M. N. Schmitt можно. Она основана на теории, сторонники которой отрицали то, что нейтрализация может предполагать нападение на военный объект не с целью его разрушения или повреждения, а с целью недопущения его использования противной стороной (Bothe et al., 1982). Надо полагать, что эта теория не отвечает реальному положению дел. Многие боевые задачи достаточно часто заключаются в том, чтобы ограничить противнику доступ к какому-либо военному объекту. Особенно это касается вооруженного конфликта в киберпространстве. Достаточно помыслить следующую возможную ситуацию: система противоракетной обороны противной стороны может быть нейтрализована на определенное время вследствие кибератаки, которая нарушит ее функционирование, но не причинит какого-либо вреда ее физической инфраструктуре. В доктрине большинство исследователей поддерживают теорию, выдвинутую K. Dörmann (Droege, 2012; Pool, 2013; Kelsey, 2008; Hathaway et al., 2012).

Обратимся теперь к Руководству. В норме 92 закреплено следующее определение кибератаки: «кибератака — это наступательная или оборонительная кибероперация, которая, как разумно ожидается, приведет к причинению травм или смерти людей, либо к повреждению или разрушению объектов» (Schmitt, 2013).

Очевидным фактом является то, что данная норма Руководства отражает точку зрения M. N. Schmitt, что не удивительно, т. к. он является редактором Руководства. Более того, в п. 2 комментария к данной норме прямо указано, что основой для нее послужил п. 1 ст. 49 Дополнительного Протокола I (Schmitt, 2013). Однако пп. 10–13 свидетельствуют о том, что разработчики Руководства не пришли к единому мнению относительно содержания понятия «повреждение объектов», в частности, входит ли в это понятие нарушение функционирования объекта (Schmitt, 2013).

В связи с этим необходимо согласиться с C. Droege (2012), которая указывает на ограничительный характер теории, предложенной М.Н. Шмиттом. Действительно, абсурдным представляется вывод, согласно которому объект, выведенный из строя кибератакой, не является поврежденным. Иными словами, будет ли разница в последствиях для гражданского населения в случае разрушения сети энергоснабжения в результате бомбардировки и в ситуации выведения этой сети из строя посредством кибератаки? По нашему мнению, последствия будут идентичными, и поэтому можно прийти к выводу, что критерий наличия физического повреждения, не является идеальным.

Разумной также выглядит ссылка C. Droege (2012) на принцип соразмерности, который предполагает наличие сопутствующего ущерба, но также предполагает защиту гражданских объектов и гражданского населения от случайного ущерба. Очевидно, что понятие «ущерб» отличается по содержанию от понятия «уничтожение». Под ущербом в указанном контексте необходимо понимать причиненный вред, в результате которого поврежденный объект теряет какие-либо свои полезные свойства. Поэтому вполне логично считать ущербом нарушение нормального функционирования различных инфраструктур в результате кибератак.

В то же самое время необходимо понимать, что нарушение нормального функционирования в киберпространстве — это явление временного характера, поскольку поврежденная система и данные в ней всегда могут быть восстановлены. По этой причине логично квалифицировать

кибератаки в качестве нападения даже в том случае, когда они привели к временному нарушению нормального функционирования инфраструктуры без ее физического разрушения или повреждения.

Вышеуказанные замечания позволяют говорить о расширительном толковании понятия «нападение» применительно к киберпространству. Тем не менее, если взять за основу расширительный подход, то можно прийти к абсурдному выводу, что все кибератаки, направленные против гражданских информационных систем, необходимо признавать нападениями по смыслу МГП. В таком случае напрочь стирается граница между кибернетическим уголовным правом и МГП. В связи с этим надо согласиться с C. Droege (2012), высказавшей опасение, что «приравнивание к нападениям таких нарушений ... выходит за границы предполагаемой сферы действия норм ведения военных действий».

M. N. Schmitt (2002; 2011), в свою очередь, в качестве критерия, позволяющего отграничить кибератаки, являющиеся нападениями по смыслу МГП, от актов киберпреступности, предлагает критерий неудобства. Но что считать неудобством? Представляется, что данный критерий является достаточно расплывчатым.

Надо полагать, что для разрешения этой проблемы поможет концепция «критической инфраструктуры», предложенная N. Melzer (2011). Более того, данный подход уже отражен в существующих договорах по информационной безопасности и некоторых национальных правовых актах (в частности, в российских)[33]. Так, в соответствующем Соглашении между Правительством Российской Федерации и Правительством Китайской Народной Республики понятие «объекты критической информационной инфраструктуры» определено наиболее полным образом: «Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети государственных органов; информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, предназначенные для обеспечения обороны страны, безопасности государства и правопорядка, а также функционирующие в области здравоохранения, транспорта, связи, в кредитно-финансовой сфере, в оборонно-промышленном и топливно-энергетическом комплексах, в атомной, ракетно-космической и химической промышленности, в отраслях промышленности с непрерывным циклом производства»[34]. Выходит, что кибератака, нарушающая нормальное функционирование именно таких объектов (без их физического разрушения), должна считаться нападением по смыслу МГП. Тем не менее при всей очевидности вывода здесь также необходима соответствующая практика государств.

[33] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. Бюллетень международных договоров, Март 1993–2012, № 1, с. 13–21; Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 г. Бюллетень международных договоров, Март 1993–2015, № 7, с. 16–23; Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. Бюллетень международных договоров, Март 1993–2016, № 11, с. 82–88; Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» Собрание законодательства Российской Федерации 2017, № 31, Статья 4736.

[34] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. Бюллетень международных договоров, Март 1993-2016, № 11, с. 82–88.

## Выводы и дискуссия

В результате проведенного исследования, было выявленно:

1. Под ограничения военных действий, установленные нормами МГП, попадают все кибероперации, которые приравниваются к таким военным действиям (*ratione materiae*).

2. Что касается вопроса о действии во времени норм МГП в киберпространстве (*ratione temporis*), то началом применения норм необходимо считать момент возникновения вооруженного конфликта, в рамках которого совершаются кибероперации, либо момент возникновения вооруженного конфликта, ограниченного киберпространством, без применения традиционной вооруженной силы. Напротив, проблема окончания применения таких норм остается в известной степени теоретической, поскольку отсутствует соответствующая практика государств.

3. Кибератака будет квалифицироваться как нападение по смыслу МГП в случаях, если она приводит к гибели людей, причинению им увечий, физическому разрушению или повреждению объектов, а также в ситуациях, когда нарушается нормальное функционирование объектов критической информационной инфраструктуры без физического их разрушения или повреждения.

Не последнюю роль в вопросах *ratione materiae* и *ratione temporis* МГП в киберпространстве, а также в вопросе квалификации кибератаки в качестве нападения по смыслу МГП играет практика государств. Более того, практика государств играет большую роль для развития соответствующих норм международного права в отношении киберпространства в целом, поэтому ее необходимо развивать.

Первой мыслью по решению вышеуказанной проблемы практики, которая приходит на ум, является предложение о разработке соответствующего международного договора. Однако, во-первых, процесс создания международного договора, как известно, достаточно продолжителен по времени. Есть вероятность, что разработка такого международного договора может занять даже не годы, а десятилетия.

Во-вторых, на сегодняшний день очевидно, что не все государства поддерживают инициативу разработки и принятия такого международного договора, достаточно вспомнить российский проект Конвенции о международной информационной безопасности, не имевший успеха при рассмотрении в ООН. Поэтому, на наш взгляд, на данный момент самым приемлемым решением остается развитие соответствующей практики государств.

## Заключение

Итак, ключевым является вывод о необходимости разработки практики государств по вопросам предметных и временных рамок применения норм международного гуманитарного права в киберпространстве, а также по вопросу правовой квалификации кибератаки. Тем не менее помимо этого очевидного вывода, представляется правильным не только ждать момента, когда соответствующая практика будет сформирована, но также, чтобы международное сообщество использовало другие способы для решения данной проблемы. В частности, необходимо вынесение этой проблемы на рассмотрение в пленарные органы международных организаций, например, в Генеральную Ассамблею Организации Объединенных Наций. По нашему мнению, целью создания такой практики и международного договора является не разработка новых норм международного гуманитарного права, которые заменят существующие, а адаптация существующих норм применительно к киберпространству.

## Список литературы / References:

1. Backstrom, A. & Henderson, I. (2012). New capabilities in warfare: An overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews. *International Review of the Red Cross*, *94*(886), 483–514.
2. Bothe, M., Partsch, K. J. & Solf, W. A. (1982). *New rules for victims of armed conflicts: Commentary to the two 1977 protocols additional to the Geneva Conventions of 1949*. Martinus Nijhoff Publishers.
3. Brown, G. D. (2011). Why Iran didn't admit Stuxnet was an attack. *Joint Force Quarterly*, *63*, 70–73.
4. Buchan, R. (2012). Cyber attacks: Unlawful uses of force or prohibited interventions? *Journal of Conflict and Security Law*, *17*(2), 211–227.
5. Danel'yan, A. A. (2020). Mezhdunarodno-pravovoe regulirovanie kiberprostranstava [International legal regulation of cyberspace]. *Obrazovanie i Pravo*, *1*, 261–269.
6. David, E. (2011). *Printsipy prava vooruzhennykh konfliktov: Kurs lektsii, prochitannykh na yuridicheskom fakultete Otkrytogo Brussel'ckogo Universiteta* [Principes de droit des conflits armés: Précis de la faculté de droit de l'Université Libre de Bruxelles]. CICR.
7. Dinniss, H. H. (2012). *Cyber warfare and the laws of war*. Cambridge University Press.
8. Dinstein, Y. (2016). *The conduct of hostilities under the law of international armed conflict* (3rd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781316389591
9. Droege, C. (2012). Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, *94*(886), 533–578.
10. Franklin, A. (2018). An international cyber warfare treaty: Historical analogies and future prospects. *Journal of Law & Cyber Warfare*, *7*(1), 149–164.
11. Geiß, R. & Lahmann, H. (2012). Cyber warfare: Applying the principle of distinction in an interconnected space. *Israel Law Review*, *45*(3), 381–399. https://doi.org/10.1017/S0021223712000179
12. Hathaway, O. A., Crootof, R., Levitz, Ph., Nix, H., Nowlan, A., Perdue, W. & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, *100*(4), 817–885.
13. Henckaerts, J.-M. & Doswald-Beck, L. (2006). *International Commitee of the Red Cross. Customary international humanitarian law. Volume I: Rules*. Cambridge University Press.
14. Kelsey, J. T. G. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. *Michigan Law Review, 106*(7), 1427–1451. https://repository.law.umich.edu/mlr/vol106/iss7/6
15. Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*(886), 515–531.
16. Melzer, N. (2017). *International humanitarian law: A comprehensive introduction*. International Commitee of the Red Cross.
17. Melzer, N. (2011). *Cyberwarfare and international law*. The United Nations Institute for Disarmament Research (UNIDIR).
18. Demeyere, B., Henckaerts, J.-M., Hiemstra, H., & Nohle, E. (2016). The updated ICRC commentary on the Second Geneva Convention: Demystifying the law of armed conflict at sea. *International Review of the Red Cross*, *98*(2), 401–417. https://doi.org/10.1017/S1816383117000376
19. Pool, P. (2013). War of the cyber world: The law of cyber warfare. *The International Lawyer*, *47*(2), 299–323.
20. Sandoz, Y., Swinarski, C. & Zimmermann, B. (Eds.). (1987). *Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. International Commitee of the Red Cross, Kluwer Academic Publishers.

21. Schmitt, M. N. (2019). Wired warfare 3.0: Protecting the civilian population during cyber operations. *International Review of the Red Cross*, *101*(1), 333–355.
22. Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
23. Schmitt, M. N. (2014). Rewired warfare: Rethinking the law of cyber attack. *International Review of the Red Cross*, *96*(893), 189–206.
24. Schmitt, M. N. (Eds.). (2013). *Tallinn Manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288
25. Schmitt, M. N. (2012a). "Attack" as a term of art in international law: The cyber operations context. *4th International Conference on Cyber Conflict Proceedings* (pp. 283–293). Tallinn.
26. Schmitt, M. N. (2012b). Classification of cyber conflict. *Journal of Conflict and Security Law*, *17*(2), 245–260. https://doi.org/10.1093/jcsl/krs018
27. Schmitt, M. N. (2011). Cyber operations and the jus in bello: Key issues. *Naval War College International Law Studies*, *87*, 89–110. https://digital-commons.usnwc.edu/ils/vol87/iss1/7/
28. Schmitt, M. N. (2010). Cyber operations in international law: The use of force, collective security, self-defense and armed conflict. *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy* (pp. 151–178). National Research Council, Washington D. C.
29. Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross*, *84*(846), 365–399.
30. Talimonchik, V. P. (2015). International legal means of combating information weapons. *Russian Yearbook of International Law*, Special Issue, 135–151.
31. Tikk, E., Kaska, K. & Vihul, L. (2010). *International cyber incidents: Legal considerations*. CCDCE.
32. Zhang, L. (2012). A Chinese perspective on cyber war. *International Review of the Red Cross*, *94*(886), 801–807.

**Сведения об авторе:**

**Гаркуша-Божко С. Ю.** — магистр международного права, юрисконсульт Школы высшего спортивного мастерства по водным видам спорта имени Ю. С. Тюкалова, Санкт-Петербург, Россия.
garkusha-bozhko.sergej@yandex.ru
ORCID 0000-0003-1253-3157

**Information about the author:**

**Sergey Y. Garkusha-Bozhko** — LLM in Law, Legal Advisor, School of Higher Sportsmanship in Water Sports named after Yu. S. Tyukalov, St. Petersburg, Russia.
garkusha-bozhko.sergej@yandex.ru
ORCID 0000-0003-1253-3157