УДК 341.31 Вестник СПбГУ. Право. 2023. Т. 14. Вып. 1

Определение вооруженного конфликта в киберпространстве

С. Ю. Гаркуша-Божко

Усть-Луга Ойл,
Российская Федерация, 190000, Санкт-Петербург, наб. реки Мойки, 77

Для цитирования: Гаркуша-Божко, Сергей Ю. 2023. «Определение вооруженного конфликта в киберпространстве». *Вестник Санкт-Петербургского университета. Право* 1: 194–210. https://doi.org/10.21638/spbu14.2023.112

Развитие информационных технологий затрагивает все сферы деятельности человечества, включая военную деятельность государств. Уровень развития военных информационных технологий позволяет говорить о новом театре военных действий — информационном пространстве (киберпространстве). Вероятность вооруженного конфликта в киберпространстве также подтверждает разработанное в 2013 г. и обновленное в 2017 г. специалистами из стран военно-политического блока НАТО при участии Международного комитета Красного Креста Таллинское руководство по международному праву, применимому к кибероперациям. В условиях высокой вероятности осуществления военных действий в киберпространстве отправной точкой для применения норм международного гуманитарного права к таким ситуациям является определение кибернетического вооруженного конфликта. Изучение этой актуальной проблемы стало предметом настоящей статьи. Автор уделяет внимание правовому определению киберпространства в целом и связанным с этой сферой проблемам. В связи с отсутствием международного договора, регулирующего данную сферу, высказано предложение о его разработке и принятии. Так как в международном гуманитарном праве отсутствует определение «классического» вооруженного конфликта, в статье на основе анализа норм права вооруженных конфликтов, соответствующей практики и международно-правовой доктрины предлагается его авторское определение. На основе этого определения, подробного анализа соответствующих норм международного права, в том числе норм, предложенных Таллинским руководством по международному праву, применимому к кибероперациям, доктрины международного права и с учетом особенностей киберпространства дается авторское комплексное определение вооруженного конфликта в киберпространстве. Автор обосновывает необходимость использования именно понятия кибернетического вооруженного конфликта, а не терминов «кибервойна» или «информационная война». Уделяется внимание оценке соответствующих положений Таллинского руководства. Высказаны предложения по возможному решению рассмотренных проблем.

Ключевые слова: киберпространство, вооруженный конфликт, информационные технологии, международное гуманитарное право, кибернетический вооруженный конфликт, право вооруженных конфликтов, цифровой суверенитет.

1. Введение

Развитие информационных технологий в современном мире 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 называют в западных странах, киберпространство (*англ.* cyberspace). 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 российского Президента В. В. Путина: «Одним из основных стратегических вызовов современности является риск возникновения масштабной конфронтации в цифровой сфере»[1].

Как отмечают в доктрине, киберпространство является «пятой сферой или пятым доменом ведения военных действий» после суши, моря, воздушного и космического пространств (Мельцер 2017, 51). Данное утверждение не может быть оспорено, поскольку в силу уровня развития современных технологий киберпространство — это потенциальный театр военных действий. Высокая вероятность таких вооруженных конфликтов заставила государства задуматься о вопросе их правового регулирования, и в 2013 г. благодаря усилиям юристов и военных специалистов из стран военно-политического блока НАТО при участии специалистов из Международного комитета Красного Креста (МККК) было разработано Таллинское руководство по международному праву, применимому к кибервооружениям[2] (далее — Таллинское руководство, Руководство). Руководство стало попыткой разработать нормы международного права, применимые не только к указанному роду вооруженных конфликтов, но и к киберпространству в целом как в военное, так и в мирное время. Необходимость этих международно-правовых норм очень высока, что и обусловило принятие новой расширенной версии Руководства в 2017 г.[3] Существование Руководства лишний раз доказывает актуальность проблемы правового регулирования как вооруженных конфликтов в киберпространстве, так и киберпространства в целом.

Конечно, в случае начала вооруженного конфликта в киберпространстве к нему будут применяться нормы международного гуманитарного права (МГП). Однако отправной точкой для применения норм МГП к киберпространству является определение вооруженного конфликта в киберпространстве (кибернетического вооруженного конфликта). Попытаемся разобраться в этом непростом вопросе, но сначала рассмотрим вопрос правового определения киберпространства.

---

[1] Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности от 25.09.2020. Дата обращения 7 марта, 2021. http://kremlin.ru/events/president/news/64086.

[2] Tallinn Manual on the International Law Applicable to Cyber Warfare. 2013. Дата обращения 7 марта, 2021. http://csef.ru/media/articles/3990/3990.pdf.

[3] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2017. Дата обращения 7 марта, 2021. https://books.google.ru/books?id=n9wcDgAAQBAJ&lpg=PR12&lr&pg=PA196#v=onepage&q&f=false (далее ссылки на страницы этой версии даются в тексте).

2. Основное исследование

2.1. Понятие киберпространства

Термин «киберпространство» имеет не такую длинную историю, так как введен в научный оборот сравнительно недавно. Интересно, что его автором был не ученый, а американо-канадский писатель-фантаст У. Гибсон, который впервые использовал данный термин в 1982 г. в рассказе «Сожжение Хром» (*англ.* Burning Chrome), а потом в 1984 г. в романе «Нейромант» (*англ.* Neuromancer) (Невский 2017).

Если оценить понятие «киберпространство» с лингвистической точки зрения, то очевидна его связь с кибернетикой. Как известно, предметом изучения этой науки выступают общие закономерности процессов управления и передачи информации (Игнатьев 2016, 6). Таким образом, киберпространство — это явление информационных технологий, правовое регулирование которых на сегодняшний день представляет собой актуальнейший вопрос правовой науки в целом. Поэтому вполне уместным синонимом понятия «киберпространства» будет понятие «информационное пространство».

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 ст. 2 концепции Конвенции об обеспечении международной информационной безопасности[4], 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, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию. Представляется, что данное определение является достаточно общим и не отражает в полной мере международную составляющую киберпространства. Более того, российская инициатива по принятию международного договора в сфере информационной безопасности не нашла должной поддержки. Так, США и западноевропейские страны отрицают необходимость принятия подобного международного договора (Croft 2012; Дрёге 2012, 4).

Аналогичное определение закреплено в соглашениях о сотрудничестве в области обеспечения международной информационной безопасности между Правительствами государств — членов Шанхайской организации сотрудничества от 16.06.2009, между Правительством РФ и Правительством Республики Беларусь от 25.12.2013 и между Правительством РФ и Правительством Китайской Народной Республики от 08.05.2015[5].

---

[4] Конвенция об обеспечении международной информационной безопасности (концепция). *Министерство иностранных дел РФ.* 2011. Дата обращения 7 марта, 2021. https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

[5] Здесь и далее, если не указано иное, все ссылки на российские, международные нормативно-правовые акты и судебную практику приводятся по СПС «КонсультантПлюс». Дата обращения 7 марта, 2021. http://www.consultant.ru.

Достаточно интересное определение находим в ст. 1 Соглашения от 19.05.2011 о создании информационной инфраструктуры инновационной деятельности государств — участников СНГ в форме распределенной информационной системы и портала СНГ «Информация для инновационной деятельности государств — участников СНГ: информационное пространство — совокупность информационных ресурсов, информационных систем и технологий, информационно-телекоммуникационной инфраструктуры, обеспечивающих информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей».

В Таллинском руководстве 2.0 под киберпространством понимается среда, образованная физическими и нефизическими компонентами для хранения, модификации и обмена данными с использованием компьютерных сетей (с. 564). Настоящее определение представляется достаточно точным и основано на научно-техническом определении киберпространства. Однако оно закреплено не в нормативной части Руководства, а в разделе «Словарь» в конце Руководства, т. е., по сути, не имеет характера нормы-дефиниции.

Также можно выделить определение, разработанное совместной группой российских и американских специалистов, которые занимались разработкой критически важных определений в киберсфере. В частности, они отметили, что под киберпространством понимается электронная среда, в которой информация создается, передается, принимается, хранится, обрабатывается и уничтожается[6]. Данное определение отражает саму суть киберпространства, но оно, как и другие указанные определения, не учитывает важного момента, который очень важен для международно-правового определения понятия «киберпространство». Речь идет о глобальном характере киберпространства, который обеспечивает возможность информационного обмена и взаимодействия, невзирая 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[7], принятый в России в 2019 г., иллюстрирует данную тенденцию.

Однако не следует отождествлять интернет и киберпространство, так как установление суверенитета над национальными сегментами интернета — это только один из аспектов установления суверенитета над киберпространством. Глобальная сеть Интернет не тождественна киберпространству, как многие ошибочно считают. Киберпространство включает в себя глобальную сеть Интернет, но не ограничивается ею. В подтверждение можно привести определение киберпространства, закрепленное в Доктрине информационной безопасности РФ, утв. Указом Президента РФ от 05.12.2016 № 646, в которой данное понятие именуется «информационной сферой». В доктрине под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информа-

[6] The Russia — U.S. Bilateral on Cybersecurity. Critical Terminology Foundations. Issue 1. Дата обращения 7 марта, 2021. https://issuu.com/ewipublications/docs/russia-us-terminology.

[7] Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации"».

ционных 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 отношений. Как видно из данного определения, интернет не тождествен киберпространству. Отдельные авторы также отмечают, что киберпространство включает в себя глобальную сеть Интернет, но ею не ограничивается (Данельян 2020, 262). Исходя из приведенного определения, киберпространство представляет собой совокупность компьютерных сетей, мобильных устройств и пользователей, которые взаимодействуют между собой на расстоянии, а интернет является связующим каналом для такого взаимодействия.

Доктрина информационной безопасности РФ также подтверждает наличие тенденции к установлению государственного суверенитета в информационной сфере (цифровой суверенитет). В связи с этим важно определить, какие области киберпространства попадают под суверенитет государства. Так, по мнению А. А. Стрельцова, в киберпространстве можно выделить три основные области верховенства государства (Стрельцов 2015, 156); к ним относятся: 1) электронная среда сбора, передачи, хранения и обработки информации, образуемая совокупностью сетей средств вычислительной техники, сетей средств связи и коммуникации и сетей средств хранения информации, расположенных на национальной территории; 2) информационно-коммуникационные технологии (ИКТ), определяющие методы и способы использования электронной среды для удовлетворения потребностей конкретного субъекта киберпространства (гражданина, юридического лица, государства, включая его органы, субъектов вооруженных конфликтов, а также преступных, включая террористических, организаций), связанных со сбором, передачей, хранением, получением или распространением информации; 3) локальные или распределенные информационные системы, системы автоматизированного управления производствами и деятельностью людей (Стрельцов 2015, 156–157).

Если внимательно проанализировать указанные области киберпространства, в которых государство осуществляет свой цифровой суверенитет, то можно вывести принципы, на которых он основан, — это принципы территориального верховенства, национальной (гражданской) принадлежности и защиты национальных интересов. Иными словами, государство имеет право осуществлять свой цифровой суверенитет над инфраструктурой киберпространства, лицами в киберпространстве и кибердеятельностью в случае, если эти составляющие киберпространства находятся под его юрисдикцией в силу территориального верховенства или наличия его гражданства (национальности), либо в случае, когда указанные составляющие затрагивают национальные интересы такого государства, например интересы его национальной безопасности.

Данный вывод подтверждается рядом норм, предложенных в Таллинском руководстве. Прежде всего, это норма 2: «Государство обладает суверенной властью в отношении киберинфраструктуры, лиц и кибердеятельности, расположенных на его территории, при условии соблюдения своих международно-правовых обязательств» (с. 13). Согласно норме 8 «с учетом ограничений, установленных международным правом, государство может осуществлять территориальную и экстерриториальную юрисдикцию в отношении кибердеятельности» (с. 51). Норма 9 конкретизирует положения о территориальной юрисдикции государства в ки-

берпространстве: «Государство может осуществлять территориальную юрисдикцию в отношении: a) киберинфраструктуры и лиц, занимающихся кибердеятельностью на его территории; b) кибердеятельности, начавшейся на его территории или завершившейся на ней; или c) кибердеятельности, имеющей существенное влияние на его территорию» (с. 55). Положения об экстерриториальной юрисдикции закреплены в норме 10: «Государство может осуществлять экстерриториальную предписывающую юрисдикцию в отношении кибердеятельности: a) проводимой его гражданами; b) совершенной на борту судов и воздушных судов, имеющих его национальность; c) проводимой иностранными гражданами и направленной на серьезный подрыв существенных интересов [такого] государства; d) проводимой иностранными гражданами против граждан [такого государства], с определенными ограничениями; или e) которая представляет собой преступления по международному праву, подпадающие под действие принципа универсальности» (с. 60).

В числе оснований для осуществления цифрового суверенитета норма 10 указывает также принцип универсальной юрисдикции. Данное предложение разработчиков Таллинского руководства вполне обоснованно, так как государство должно иметь право преследовать лицо за совершение преступления по международному праву в соответствии с этим принципом и в киберпространстве — это отвечает целям международного права.

Таким образом, цифровой суверенитет государства основан на тех же классических принципах территориального верховенства, национальной (гражданской) принадлежности, защиты национальных интересов и универсальной юрисдикции. Данное умозаключение важно для более полного международно-правового определения киберпространства.

Вместе с тем не все исследователи поддерживают концепцию распространения государственного суверенитета на киберпространство. В частности, А. А. Стрельцов критикует территориальную привязку информационной инфраструктуры как основание цифрового суверенитета. По его мнению, поскольку вопросом по поддержанию и развитию системы распределения и использования цифрового адресного пространства (системы доменных имен) занимается некоммерческая организация Internet Corporation for Assigned Names and Numbers (ICANN), учрежденная в США, сложилась ситуация, в которой США де-факто распространили государственный суверенитет на регулирование вопросов обеспечения единства глобальной электронной среды, устойчивости соединения национальных электронных сред, а также информационного взаимодействия граждан различных государств, использования ресурсов национальных информационных инфраструктур для выполнения ИКТ в интересах субъектов различных сфер жизни общества. Кроме того, не все государства обладают возможностью установления цифрового суверенитета (Стрельцов 2015, 158).

Позволим себе не согласиться с таким мнением. Сфера распределения доменных имен, которой занимается ICANN, в большей мере относится к глобальной сети Интернет. Выше мы уже отмечали, что киберпространство не ограничивается интернетом, поэтому нельзя с полной уверенностью говорить, что ICANN регулирует все киберпространство. Конечно, мы принимаем во внимание, что некоммерческая организация ICANN образована в соответствии с Законом о некоммер-

ческих благотворительных корпорациях американского штата Калифорния[8], что создает риски попыток со стороны Правительства США контролировать эту организацию. Однако 01.10.2016 истек срок действия контракта ICANN с Министерством торговли США и Национальным управлением информации и связи США, в результате чего администрирование адресного пространства интернета полностью перешло под контроль ICANN[9], что снижает такой риск.

Учитывая факт истечения срока данного контракта, важно также понимать, что риск нивелировался незначительно: маловероятно, что в такой важной сфере Соединенные Штаты не попытались бы контролировать юридическое лицо, которое учреждено по закону одного из штатов США. Вместе с тем такое поведение Соединенных Штатов на мировой арене не в новинку — США всегда пытаются извлечь для себя выгоду, невзирая на нормы международного права, но это не повод подстраиваться под американские интересы. Поэтому государства и пытаются осуществлять цифровой суверенитет в киберпространстве.

В этом смысле странным выглядит заявление А. А. Стрельцова о том, что полномочия ICANN по администрированию системы доменных имен являются международным обычаем (Стрельцов 2015, 157). Стремление государств осуществлять цифровой суверенитет опровергает данный тезис и дает основания говорить о формировании новой обычной нормы международного права — нормы о цифровом суверенитете государства. Закрепление указанной нормы в Таллинском руководстве лишний раз подтверждает это. Вдобавок полномочия вышеуказанной американской корпорации — следствие того, что развитие информационных технологий в США происходило быстрее, чем в других государствах. В частности, родиной интернета, как известно, являются именно США, поэтому появление такой организации в США вполне обоснованно. Однако с момента становления интернета как глобальной мировой информационной сети государства стали задумываться о независимом международном регулировании данного явления, стали звучать заявления о необходимости создания международной организации в сфере регулирования интернета, основанной на равноправном участии государств[10]. Такие инициативы еще раз подтверждают стремление государств к защите цифрового суверенитета.

Что касается второго аргумента А. А. Стрельцова, то доля правды в нем есть: не все государства в состоянии активно защищать цифровой суверенитет, но это не повод вовсе отказываться от защиты. Ведущие страны активно отстаивают свой суверенитет в киберсфере, это глобальный тренд, обусловленный самим существованием государств: они всегда будут пытаться осуществлять суверенитет в любой сфере, где это допускают нормы международного права, включая киберпространство. Поэтому на данный момент одной из особенностей киберпространства явля-

[8] Amended and restated Articles of Incorporation of Internet Corporation for Assigned Names and Numbers. Approved by the ICANN Board on 9 August 2016, and filed with the California Secretary of State on 3 October 2016. Дата обращения 7 марта, 2021. https://www.icann.org/resources/pages/governance/articles-en.

[9] «США лишились возможности влиять на мировое управление интернетом». *Lenta.ru.* 2016. Дата обращения 7 марта, 2021. https://lenta.ru/news/2016/10/02/noinetusa.

[10] «Медведев: РФ поддерживает создание международной организации по регулированию интернета». *ТАСС.* 2021. Дата обращения 7 марта, 2021. https://tass.ru/ekonomika/2531411/amp.

ется то, что в нем существуют области, на которые распространяется юрисдикция государств (суверенитет).

Вместе с тем киберпространство — это глобальное пространство, где границы такого государственного суверенитета весьма относительны — глобальное информационное взаимодействие находится вне государственных границ. Киберпространство имеет двойственный характер: с одной стороны, оно глобально и в нем отсутствуют государственные границы, а с другой — формирующиеся нормы международного права разрешают осуществлять государствам юрисдикцию в этом пространстве в установленных такими нормами случаях. Указанную природу киберпространства необходимо учитывать при выработке его международно-правового определения.

Исходя из отсутствия универсального международно-правового определения киберпространства, попытаемся дать такое определение с учетом проведенного анализа. *Киберпространство* — это глобальная электронная среда, образованная физическими и нефизическими компонентами, включая комплекс технических и программных средств, в которой посредством использования компьютерных и мобильных сетей, включая глобальную информационно-коммуникационную сеть Интернет, осуществляются формирование, передача, прием, хранение, обработка, модификация и уничтожение информации. Государства имеют право осуществлять свой суверенитет в киберпространстве на основе принципов территориального верховенства, национальной (гражданской) принадлежности, защиты национальных интересов и универсальной юрисдикции.

Предложенный вариант определения является попыткой отразить как технический, так и правовой аспекты киберпространства. Полагаем, нужно разработать на уровне ООН международный договор о регулировании киберпространства, так как его отсутствие создает ощутимые проблемы в международно-правовом регулировании данной сферы, в частности в вопросе международно-правового определения киберпространства.

2.2. Понятие вооруженного конфликта

Прежде чем перейти к определению кибернетического вооруженного конфликта, необходимо дать определение понятия вооруженного конфликта в традиционном правовом смысле. Вспомним замечание известного французского юриста-международника Ш. Руссо о том, что вооруженный конфликт — это действие-условие, которое влечет за собой применение определенного правового статуса (Rousseau 1983, 7).

В международном гуманитарном праве используется термин «вооруженный конфликт», а не «война». Причины этого можно найти в комментарии к Первой Женевской конвенции от 12.08.1949[11] об улучшении участи раненых и больных в действующих армиях, подготовленном одним из самых известных специалистов в области МГП — швейцарским юристом Ж. Пикте, который многие годы входил в состав руководства МККК. В частности, в комментарии к ст. 2, общей для всех Женевских конвенций, Ж. Пикте отметил: «Замена термина “война” на гораздо бо-

[11] Женевские конвенции от 12 августа 1949 года и Дополнительные протоколы к ним. 2011. 5-е изд., доп. М.: Международный комитет Красного Креста.

лее широкое понятие "вооруженный конфликт" была намеренной. Можно почти бесконечно спорить о юридическом определении "войны". Государство, совершая враждебное действие по отношению к другому государству, всегда может притвориться, что оно не ведет войну, а всего лишь проводит полицейскую акцию или действует в рамках правомерной самообороны. Выражение "вооруженный конфликт" затрудняет такие споры. Любые разногласия, возникающие между государствами и ведущие к вмешательству вооруженных сил, являются вооруженным конфликтом… даже если одна из сторон отрицает существование состояния войны» (Pictet 1952, 32).

Следовательно, причины замены традиционного понятия «война» на более широкое понятие «вооруженный конфликт» были сугубо практические: концепция вооруженного конфликта охватывает намного больше ситуаций, чем термин «война»; выбор более широкого понятия позволяет решить проблему белых пятен в правовом регулировании всевозможных вооруженных столкновений. Такой подход находит поддержку среди специалистов по международному гуманитарному праву (Сассоли, Бувье 2008, 117; Давид 2011, 111). Так, известный бельгийский юрист Э. Давид отмечает: «Говорить о праве войны, придавая такой узкий смысл слову "война", — значит, вступать в противоречие с тем фактом, что вооруженная борьба между лицами, не отвечающая приведенному выше определению, все же относится к ведению права… войны» (Давид 2011, 112).

Широкий смысл понятия «вооруженный конфликт» закреплен в тексте Женевских конвенций: согласно ч. 1 ст. 2, общей для Женевских конвенций, указанные конвенции применяются не только к случаям объявленной войны, но и к случаям «всякого *другого* вооруженного конфликта, возникающего между двумя или несколькими Высокими Договаривающимися Сторонами, даже в том случае, если одна из них *не признает состояния войны* (курсив мой. — *С. Г.-Б.*)». Данное положение лишний раз подтверждает более широкий характер термина «вооруженный конфликт».

Современные международные договоры и иные международные акты не содержат понятия «война» — разработчики намеренно избегают его использования, применяя более широкий термин «вооруженный конфликт» (например, в ст. 18 Конвенции о защите культурных ценностей в случае вооруженного конфликта от 14.05.1954, ст. 1 Первого Дополнительного протокола к Женевским конвенциям, ст. 1 Второго Дополнительного протокола к Женевским конвенциям и различных резолюциях Генеральной Ассамблеи ООН, например Резолюции от 14.12.1974 № 3318 (XXIX), которой была принята Декларация о защите женщин и детей в чрезвычайных обстоятельствах и в период вооруженных конфликтов).

Такая логика применима и к киберпространству: с юридической точки зрения правильнее использовать понятие «вооруженный конфликт в киберпространстве» или «кибернетический вооруженный конфликт», а не «кибервойна» или «информационная война», так как первое понятие намного шире второго. Однако, несмотря на безупречность такой логики, многие исследователи ошибочно используют термины «кибервойна» и «информационная война» (Zhang 2012, 801; Дрёге 2012, 1; Шмитт 2002, 121; Pool 2013, 299; Döge 2010, 486). Кроме того, использованию понятий «кибервойна» и «информационная война» способствуют сами государства,

активно применяя их в разрабатываемых международно-правовых документах[12]. Мы придерживаемся мнения, что использование таких терминов не является юридически корректным.

Вернемся к определению традиционного вооруженного конфликта. Ни в Женевских конвенциях, ни в иных международных договорах в сфере международного гуманитарного права не содержится определения вооруженного конфликта. Это достаточно странно, ибо вооруженный конфликт имеет ключевое значение для применения норм МГП. Именно начало вооруженного конфликта является основанием для применения к таким ситуациям норм международного гуманитарного права.

Определение вооруженного конфликта можно найти в работах Комиссии международного права ООН (КМП ООН), в частности в Проектах статей о последствиях вооруженных конфликтов для международных договоров. В соответствии со ст. 2 указанных Проектов статей под вооруженным конфликтом понимается состояние войны или конфликт, сопряженный с военными действиями, которые в силу своего характера или масштабов могут затронуть действие договоров между государствами — сторонами вооруженного конфликта или между государством — стороной вооруженного конфликта и третьим государством, независимо от официального объявления войны или иного объявления какой-либо стороной или всеми сторонами вооруженного конфликта[13]. В комментарии к этому определению КМП ООН отметила, что оно основано на определении, предложенном Международным трибуналом по бывшей Югославии (МТБЮ) в апелляционном решении по юрисдикции в знаменитом деле Тадича.

В данном решении Апелляционная камера МТБЮ пришла к следующему выводу: «Вооруженный конфликт имеет место всякий раз, когда государства прибегают к силе или когда происходит продолжительный вооруженный конфликт между правительственными силами и организованными вооруженными группами или же между такими группами внутри одного государства»[14]. На основе этого определения и на основе норм международного гуманитарного права в доктрине приходят к выводу, что понятие «вооруженный конфликт» включает в себя несколько типов вооруженных конфликтов (Давид 2011, 144–145; Вите 2009, 93–97, 100–110).

Во-первых, это вооруженный конфликт международного характера (международный вооруженный конфликт), понятие которого настолько гибкое и широкое, что любое самое незначительное столкновение вооруженных сил двух и более различных государств будет рассматриваться в качестве такого конфликта.

Во-вторых, это вооруженный конфликт немеждународного характера (немеждународный вооруженный конфликт), регулируемый в первую очередь ст. 3, общей для Женевских конвенций. Его необходимым условием является то, что в его ходе друг другу должны противостоять организованные вооруженные группы (силы), находящиеся под ответственным командованием, а военные действия должны но-

[12] См. указанные выше соглашения о сотрудничестве в области обеспечения международной информационной безопасности.

[13] Draft articles on the effects of armed conflicts on treaties, with commentaries. Adopted by the ILC in 2011. Дата обращения 7 марта, 2021. https://legal.un.org/docs/?path=../ilc/texts/instruments/english/commentaries/1_10_2011.pdf&lang=EF.

[14] Prosecutor v. Dusko Tadić. Case No. IT-94-1-T.ICTY Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction of 2 October 1995. Дата обращения 7 марта, 2021. https://www.icty.org/x/cases/tadic/acdec/en/51002.htm.

сить открытый и коллективный характер. Еще одно необходимое условие признания наличия подобного вооруженного конфликта — то, что такая ситуация достигает уровня, отличающего ее от иных форм насилия, к которым МГП не применяется, например случаи нарушения внутреннего порядка и возникновения обстановки внутренней напряженности, внутренние беспорядки, отдельные спорадические акты насилия и т. п. Такой порог напряженности намного выше, чем для немеждународного вооруженного конфликта. Поскольку нормы МГП не дают прямого ответа на вопрос о том, когда подобный порог достигнут, этот вопрос остается на усмотрение судебной практики. В рассмотренном выше апелляционном решении о юрисдикции в деле Тадича МТБЮ указывает, что такой порог достигается тогда, когда ситуация может быть квалифицирована как «продолжающееся длительное время вооруженное насилие»[15]. Далее МТБЮ отмечает, что оценка ситуации на предмет наличия «продолжающегося длительное время вооруженного насилия» должна производиться исходя из двух критериев: напряженности насилия и организованности сторон[16]. Эти критерии не абстрактны и требуют отдельной оценки применительно к каждой конкретной ситуации вооруженного столкновения.

Наконец, это вооруженный конфликт немеждународного характера, речь о котором идет в п. 1 ст. 1 Второго Дополнительного протокола к Женевским конвенциям. Он отличается от предыдущего тем, что к неправительственным вооруженным группам, помимо требований организованности и нахождения под ответственным командованием, выдвигается требование об осуществлении контроля над частью территории государства, где идет такой вооруженный конфликт, который позволяет им осуществлять непрерывные и согласованные военные действия и применять Второй Дополнительный протокол. Данный тип вооруженного конфликта толкуется очень узко, к этой разновидности можно отнести только гражданскую войну, в которой противостоящими сторонами конфликта являются правительственные вооруженные силы и мятежники, имеющие постоянный контроль над частью государственной территории.

Таким образом, можно дать следующее определение вооруженного конфликта: *вооруженный конфликт* — 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 которых превышает уровень напряженности в ситуациях нарушения внутреннего порядка и возникновения обстановки внутренней напряженности, в частности в ситуациях внутренних беспорядков, отдельных спорадических актов насилия и иных аналогичных актов.

Отсутствие подобного определения в международных договорах создает некоторые трудности, поэтому очевидный выход из ситуации — внесение соответствующих поправок в международные договоры.

---

[15] Prosecutor v. Dusko Tadić. Case No. IT-94-1-T.ICTY Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction of 2 October 1995. Дата обращения 7 марта, 2021. https://www.icty.org/x/cases/tadic/acdec/en/51002.htm.

[16] Prosecutor v. Dusko Tadić. Case No. IT-94-1-T.ICTY Trial Chamber Judgment of 7 May 1997. Дата обращения 7 марта, 2021. https://www.icty.org/x/cases/tadic/tjug/en/tad-tsj70507JT2-e.pdf.

2.3. Вооруженный конфликт в киберпространстве

Таллинское руководство не содержит отдельной нормы — дефиниции вооруженного конфликта в киберпространстве, однако такое определение имеется в п. 2 комментария к норме 80, где указано, что кибероперации, осуществляемые в контексте вооруженного конфликта, попадают под действие права вооруженных конфликтов (с. 375). Исходя из этого, в Таллинском руководстве под вооруженным конфликтом понимается ситуация, связанная с осуществлением военных действий, включая действия с использованием киберсредств. В подстрочной ссылке к данному определению со ссылкой на общую ст. 2 Женевских конвенций указано, что в качестве вооруженного конфликта также будет квалифицироваться ситуация оккупации, в которой отсутствует вооруженное сопротивление (с. 375). Далее говорится о том, что понятие «вооруженный конфликт» приобретает различное значение в зависимости от его типологии, закрепленной в нормах 82 и 83 Руководства (с. 375–376).

Согласно норме 82 «международный вооруженный конфликт имеет место всякий раз, когда между двумя или более государствами происходят военные действия, которые могут включать кибероперации или ограничиваться ими» (с. 379). Норма 83 закрепила следующие положения: «Немеждународный вооруженный конфликт возникает всякий раз, когда имеет место продолжительное вооруженное насилие, которое может включать кибероперации 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» (с. 385).

Определение, закрепленное в комментарии к норме 80 Таллинского руководства, основано на нормах международного гуманитарного права и отражает суть вооруженного конфликта, но в то же время является достаточно общим. Ключевой момент в данном определении — то, что такой конфликт осуществляется с *использованием киберсредств*. Под киберсредствами необходимо понимать различные инструменты и методы, используемые в киберпространстве, на что указывает и доктрина (Lin 2012, 517).

Предлагается две классификации таких инструментов и методов (Lin 2012, 517): во-первых, киберсредства можно разделить на автономные, способные работать без вмешательства человека, и на управляемые, которые работают под контролем оператора. Во-вторых, их можно разделить на наступательные и оборонительные. Очевидно, что первая классификация основана на техническом аспекте — как известно, в информационных технологиях существуют автономные системы, работающие без вмешательства человека, а также системы, управляемые оператором. Вторая классификация, в свою очередь, основана на военном аспекте. Данные классификации пересекаются: автономные и управляемые киберсредства могут быть как оборонительными, так и наступательными. Рассмотрим сначала автономные средства, а потом управляемые.

Автономное наступательное киберсредство включает три необходимых компонента:

— доступ, т. е. инструменты и методы, с помощью которых стороны конфликта получают информацию; в рамках киберпространства распространен удаленный доступ, не требующий близкого контакта между сторонами, что значительно отличает традиционный вооруженный конфликт от кибернетического;

— различные технические уязвимости информационной системы, позволяющие ее взломать и получить доступ к информации; сделать киберсистему полностью неуязвимой невозможно, однако техническая уязвимость может быть оставлена намеренно и представлять собой ловушку для другой стороны вооруженного конфликта — в таком случае вполне уместно говорить о таком явлении, как военно-техническая хитрость;

— так называемая полезная нагрузка — механизм воздействия на информационную систему после проникновения в нее в результате использования ее технической уязвимости; например, в компьютерном вирусе полезная нагрузка — это вредоносные действия такого вредоносного программного обеспечения; более того, компьютерные вирусы — это и есть автономное наступательное киберсредство, так как они действуют самостоятельно, и в ходе вооруженного конфликта в киберпространстве одна из сторон может использовать их в целях взлома информационной системы противника и сбора в ней информации о противнике.

Принцип работы автономных оборонительных киберсредств основан на использовании одного или нескольких вышеуказанных компонентов. Например, принцип работы брандмауэра (файрвола) заключается в противодействии несанкционированному доступу в информационную систему, основанному на использовании технических уязвимостей такой системы.

С управляемыми киберсредствами дело обстоит проще: так как управляет таким инструментом оператор-человек, то объектом воздействия будет именно он; здесь применяются традиционные методы (подкуп, вербовка и т. п.). Оборонительными методами выступают различные мероприятия по предотвращению этих действий в отношении оператора. Такой подход не оспаривается в доктрине (Lin 2012, 518), однако некоторые исследователи используют в отношении киберсредств термин «кибероружие», или «информационное оружие» (Талимончик 2015, 135; Franklin 2018; Hathaway et al. 2012, 839–841; Pool 2013, 300–303). Понятие «кибероружие» является более узким, поэтому целесообразнее использовать термин «киберсредства».

Доктрина исходит из того, что все кибероперации можно разделить на кибератаки и киберэксплуатацию (Lin 2012, 518) (с. 415, 564).

В соответствии с нормой 92 Таллинского руководства кибератака — это наступательная или оборонительная кибероперация, которая, как разумно ожидается, приведет к причинению травм или смерти людей либо к повреждению или разрушению объектов (с. 415).

Киберэксплуатация — это кибероперации, направленные на проникновение в информационные системы противника с целью получения информации и не нарушающие целостность и нормальное функционирование таких систем. Как разумно отмечают в доктрине, лучшая киберэксплуатация незаметна для пользователей информационной системы, в которую осуществляется проникновение (Lin 2012, 519). Поэтому один из примеров такой кибероперации — это кибершпионаж.

В прессе порой отдельные кибероперации называют кибератаками, хотя такие кибероперации представляют собой киберэксплуатацию.

Положение Таллинского руководства о распространении понятия кибернетического вооруженного конфликта на ситуации оккупации, не встречающей вооруженного сопротивления, может показаться немного странным, так как сложно представить оккупацию в киберпространстве. Однако это впечатление ошибочно: вполне вероятна оккупация территории, где находятся серверы определенной информационной системы, которую пытаются взломать с помощью кибератаки. Именно такие ситуации предполагает данное положение Руководства, что полностью отвечает целям и принципам международного гуманитарного права.

С замечанием Таллинского руководства о том, что понятие «вооруженный конфликт» приобретает различное значение в зависимости от его типологии, мы согласны лишь частично. Международный вооруженный конфликт отличается от немеждународного в вопросе их правового регулирования, однако и международный, и немеждународный вооруженный конфликт — частные случаи более общего понятия «вооруженный конфликт». Различное правовое регулирование частных случаев не исключает их из объема общего понятия: и международный, и немеждународный вооруженный конфликт в киберпространстве остается вооруженным конфликтом в общем его понимании.

Относительно норм 82 и 83 Таллинского руководства отметим, что анализ проблемы типологии кибернетических вооруженных конфликтов заслуживает отдельной научной статьи.

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 которых 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 друг против друга.

3. Выводы

Определение кибернетического вооруженного конфликта является основой для применения международного гуманитарного права к киберпространству. Отсутствие такого определения и определения «классического» вооруженного конфликта в международных договорах создает определенные проблемы. Очевидным их решением будет внесение соответствующих поправок в существующие международные договоры по международному гуманитарному праву. Кроме того, ввиду стремительного развития информационных технологий актуален вопрос о разработке и подписании международного договора в этой сфере. В таком договоре можно отразить и вопросы правового регулирования кибернетических вооруженных конфликтов.

Библиография

Вите, Сильван. 2009. «Типология вооруженных конфликтов в международном гуманитарном праве: правовые концепции и реальные ситуации». *Международный журнал Красного Креста* 91 (873): 91–126.

Давид, Эрик. 2011. *Принципы права вооруженных конфликтов: курс лекций*. М.: Международный комитет Красного Креста.

Данельян, Андрей А. 2020. «Международно-правовое регулирование киберпространства». *Образование и право* 1: 261–269.

Дрёге, Кордула. 2012. «Слезай с моего облака: кибернетическая война, международное гуманитарное право и защита гражданских лиц». *Международный журнал Красного Креста* 94 (886): 1–60.

Игнатьев, Михаил Б. 2016. *Просто кибернетика*. СПб.: СТРАТА.

Мельцер, Нильс. 2017. *Международное гуманитарное право: общий курс*. М.: Международный комитет Красного Креста.

Невский, Борис. 2017. «Уильям Гибсон. Отец киберпространства». *Мир фантастики*. Дата обращения 7 марта, 2021. https://www.mirf.ru/book/william-gibson-otets-kiberprostranstva.

Сассоли, Марко, Антуан Бувье. 2008. *Правовая защита во время войны. Прецеденты, документы и учебные материалы, относящиеся к современной практике международного гуманитарного права*. В 4 т., т. 1: *Международное гуманитарное право: краткий очерк*. М.: Международный комитет Красного Креста.

Стрельцов, Анатолий А. 2015. «Применение международного гуманитарного права к вооруженным конфликтам в киберпространстве». *Российский ежегодник международного права*. Специальный выпуск: 152–169.

Талимончик, Валентина П. 2015. «Международно-правовые средства борьбы с информационным оружием». *Российский ежегодник международного права*. Специальный выпуск: 135–143.

Шмитт, Михель Н. 2002. «Электронная война: нападение на компьютерные сети и jus in bello». *Международный журнал Красного Креста* 846: 121–162.

Croft, Adrian. 2012. "Russia says many states arming for cyber warfare". *Reuters*. Дата обращения 7 марта, 2021. https://www.reuters.com/article/germany-cyber/russia-says-many-states-arming-for-cyber-warfare-idUSL6E8FP40M20120425.

Döge, Jenny. 2010. "Cyber warfare. Challenges for the applicability of the traditional laws of war regime". *Archiv des Völkerrechts* 48 (4): 486–501.

Franklin, Alexi. 2018. "An International Cyber Warfare Treaty: Historical analogies and future prospects". *Journal of Law & Cyber Warfare* 7 (1): 149–164.

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel. 2012. "The Law of Cyber-Attack". *California Law Review* 100 (4): 817–885.

Lin, Herbert. 2012. "Cyber conflict and international humanitarian law". *International Review of the Red Cross* 94 (886): 515–531.

Pictet, Jean S., ed. 1952. *Geneva Convention (I) for the Amelioration of the Condition of the Wounded in Armies in the Field Commentary*. Geneva: International Committee of the Red Cross.

Pool, Phillip. 2013. "War of the cyber world: The Law of Cyber Warfare". *The International Lawyer* 47 (2): 299–323.

Rousseau, Charles. 1983. *Le droit des conflits armés*. Paris: Editions A. Pedone.

Zhang, Li. 2012. "A Chinese perspective on cyber war". *International Review of the Red Cross* 94 (886): 801–807.

Статья поступила в редакцию 7 марта 2021 г.;
рекомендована к печати 28 октября 2022 г.

Контактная информация:

Гаркуша-Божко Сергей Юльевич — магистр права; garkusha-bozhko.sergej@yandex.ru

The definition of armed conflict in cyberspace

S. Yu. Garkusha-Bozhko

Ust-Luga Oil,
77, Moika River emb., St Petersburg, 190000, Russian Federation

For citation: Garkusha-Bozhko, Sergei Yu. 2023. "The definition of armed conflict in cyberspace". *Vestnik of Saint Petersburg University. Law* 1: 194–210. https://doi.org/10.21638/spbu14.2023.112 (In Russian)

The information technologies development affects all spheres of human activity, including the military activities of States. The level of military information technologies development allows us to talk about a new theatre of military operations — the cyberspace. The likelihood of an armed conflict in cyberspace is also confirmed by the Tallinn Manual, developed in 2013 and updated in 2017 by experts from the NATO States with the participation of the International Committee of the Red Cross. In the context of the high probability of military action in cyberspace, the starting point for applying international humanitarian law to such situations is the definition of a cyber armed conflict. The research of this topical issue of modern international law of armed conflicts is the subject of this article. The author pays attention to the legal definition of cyberspace in general, and to related problems. In the absence of an international treaty regulating this area, it was suggested that such treaty should be developed and adopted. Because there is no definition of "classic" armed conflict in international humanitarian law, this article offers the author's definition of "classic" armed conflict based on the analysis of the law of armed conflicts, relevant practice and international legal doctrine. Based on this definition, on detailed analysis of the relevant norms of international law, including the norms proposed by the Tallinn Manual on International Law Applicable to Cyber Operations, on the doctrine of international law, and taking into account the specifics of cyberspace, the author gives a comprehensive definition of armed conflict in cyberspace. The author substantiates the need to use the concept of cyber armed conflict, and not the terms "cyberwar" or "information war". This article focuses on and evaluates the relevant provisions of the Tallinn Manual. The author also made suggestions on possible solutions to the problems discussed in this article.

Keywords: cyberspace, armed conflict, information technologies, international humanitarian law, cyber armed conflict, law of armed conflicts, digital sovereignty.

References

Croft, Adrian. 2012. "Russia says many states arming for cyber warfare". *Reuters*. Accessed March 7, 2021. https://www.reuters.com/article/germany-cyber/russia-says-many-states-arming-for-cyber-warfare-idUSL6E8FP40M20120425.

Danel'ian, Andrei A. 2020. "International legal regulation of cyberspace". *Obrazovanie i pravo* 1: 261–269. (In Russian)

David, Eric. 2011. *Principes de Droit des Conflits Armés: Précis de la Faculté de Droit de l'Université Libre de Bruxelles*. Rus. ed. Moscow, Mezhdunarodnyi komitet Krasnogo Kresta Publ. (In Russian)

Döge, Jenny. 2010. "Cyber warfare. Challenges for the applicability of the traditional laws of war regime". *Archiv des Völkerrechts* 48 (4): 486–501.

Droege, Cordula. 2012. "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians". *Mezhdunarodnyi zhurnal Krasnogo Kresta* 94 (886): 1–60. (In Russian)

Franklin, Alexi. 2018. "An International Cyber Warfare Treaty: Historical analogies and future prospects". *Journal of Law & Cyber Warfare* 7 (1): 149–164.

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel. 2012. "The Law of Cyber-Attack". *California Law Review* 100 (4): 817–885.

Ignat'ev, Mikhail B. 2016. *Just cybernetics*. St Petersburg, STRATA Publ. (In Russian)

Lin, Herbert. 2012. "Cyber conflict and international humanitarian law". *International Review of the Red Cross* 94 (886): 515–531.
Melzer, Nils. 2017. *International humanitarian law: A comprehensive introduction*. Moscow, Mezhdunarodnyi komitet Krasnogo Kresta Publ. (In Russian)
Nevskii, Boris. 2017. "William Gibson. The father of cyberspace". *Mir fantastiki*. Accessed March 7, 2021. https://www.mirf.ru/book/william-gibson-otets-kiberprostranstva. (In Russian)
Pictet, Jean S., ed. 1952. *Geneva Convention (I) for the Amelioration of the Condition of the Wounded in Armies in the Field Commentary*. Geneva, International Committee of the Red Cross.
Pool, Phillip. 2013. "War of the cyber world: The Law of Cyber Warfare". *The International Lawyer* 47 (2): 299–323.
Rousseau, Charles. 1983. *Le droit des conflits armés*. Paris, Editions A. Pedone.
Sassòli, Marco, Antoine Bouvier. 2008. *How does law protect in war? Cases, documents and teaching materials on contemporary practice in international humanitarian law*. In 4 vols, vol. 1: *Outline of international humanitarian law*. Moscow, Mezhdunarodnyi Komitet Krasnogo Kresta Publ. (In Russian)
Schmitt, Michael N. 2002. "Wired warfare: Computer network attack and jus in bello". *Mezhdunarodnyi zhurnal Krasnogo Kresta* 846: 121–162. (In Russian)
Strel'tsov, Anatolii A. 2015. "Application of international humanitarian law to armed conflicts in cyberspace". *Rossiiskii ezhegodnik mezhdunarodnogo prava*. Spetsial'nyi vypusk: 152–169. (In Russian)
Talimonchik, Valentina P. 2015. "International legal means of combating information weapons". *Rossiiskii ezhegodnik mezhdunarodnogo prava*. Spetsial'nyi vypusk: 135–143. (In Russian)
Vite, Sil'van. 2009. "Typology of armed conflicts in international humanitarian law: Legal concepts and actual situations". *Mezhdunarodnyi zhurnal Krasnogo Kresta* 91 (873): 91–126. (In Russian)
Zhang, Li. 2012. "A Chinese perspective on cyber war". *International Review of the Red Cross* 94 (886): 801–807.

Received: March 7, 2021
Accepted: October 28, 2022

Author's information:

Sergei Yu. Garkusha-Bozhko — LLM; garkusha-bozhko.sergej@yandex.ru