МЕЖДУНАРОДНОЕ ГУМАНИТАРНОЕ ПРАВО

DOI: https://doi.org/10.24833/0869-0049-2021-1-70-80

Исследовательская статья
Поступила в редакцию: 27.12.2020
Принята к публикации: 14.02.2021

Сергей Юльевич ГАРКУША-БОЖКО
Школа высшего спортивного мастерства по водным видам спорта имени Ю.С. Тюкалова
Наб. Гребного канала, д. 10, стр. 1, Санкт-Петербург, 197110, Российская Федерация
garkusha-bozhko.sergej@yandex.ru
ORCID: 0000-0003-1253-3157

ПРОБЛЕМА КИБЕРШПИОНАЖА В МЕЖДУНАРОДНОМ ГУМАНИТАРНОМ ПРАВЕ

ВВЕДЕНИЕ. *Статья посвящена анализу проблемы кибершпионажа в контексте вооруженного конфликта в киберпространстве. Актуальность данного исследования, как части проблемы применения норм международного гуманитарного права в киберпространстве, подтверждается стремительным развитием информационных технологий, которые могут быть использованы в ходе вооруженного конфликта, а также наличием Таллинского руководства 2.0 по международному праву, применимому к кибероперациям.*

МАТЕРИАЛЫ И МЕТОДЫ. *Главными источниками настоящего исследования являются положения Таллинского руководства 2.0 по международному праву, применимому к кибероперациям, нормы Дополнительного протокола I от 08 июня 1977 г. к Женевским конвенциям от 12 августа 1949 г., нормы Гаагского «Положения о законах и обычаях сухопутной войны» 1907 г. и нормы обычного международного гуманитарного права. Методологию составили принципы, применяемые в юридических исследованиях, а также общенаучные и специальные методы правовых исследований (системный и формально-юридический методы).*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *Изучены положения Таллинского руководства о кибершпионаже на предмет соответствия нормам Дополнительного протокола I от 08 июня 1977 г. к Женевским конвенциям от 12 августа 1949 г., Гаагского «Положения о законах и обычаях сухопутной войны» 1907 г. и нормам обычного международного гуманитарного права. Также изучены проблемы, которые могут возникнуть в процессе возможного практического применения указанных положений Таллинского руководства.*

ОБСУЖДЕНИЕ И ВЫВОДЫ. *Отмечено, что положения Таллинского руководства 2.0 по международному праву, применимому к кибероперациям и кибершпионажу, основаны на соответствующих нормах международного права. По сути, соответствующее положение Таллинского руководства полностью скопировано с соответствующих норм МГП. Однако в результате настоящего исследования автор приходит к выводу, что такое слепое копирование не учитывает особенностей киберпространства и создает проблемы при возможном практическом применении данных положений Таллинского руководства.*

Во-первых, в силу анонимности пользователей на практике будет трудно провести разграничение между киберразведчиком и кибершпионом. Во-вторых, в силу сложностей в установлении четких государственных границ в киберпространстве (установлении границ государственного суверенитета), в том числе, обусловленных использованием технологий блокчейн и VPN, на практике невозможно достоверно установить, осуществлялся ли тайный сбор информации на территории противника, что, в свою очередь, влечет сложности в квалификации такого деяния в качестве кибершпионажа. И, наконец, в современных условиях шпионаж перестал быть явлением исключительно международных вооруженных конфликтов, и поэтому есть вероятность, что и кибершпионаж

может осуществляться не только в контексте вооруженного конфликта международного характера, но и в контексте вооруженного конфликта немеждународного характера. По результатам настоящего исследования были высказаны предложение о развитии практики государств по данному вопросу. Обсуждение вышеуказанных проблем на Генеральной Ассамблее ООН помогло бы выделить основные тренды развития такой практики. И только после того, как практика государств по данному вопросу станет более очевидной, можно ставить вопрос о разработке соответствующего международного договора, желательно на площадке ООН.

КЛЮЧЕВЫЕ СЛОВА: *кибершпионаж, эксплуатация компьютерных сетей, киберразведка, международное гуманитарное право, вооруженный конфликт, Таллинское руководство, шпионаж, разведка, кибершпион*

ДЛЯ ЦИТИРОВАНИЯ: Гаркуша-Божко С.Ю. Проблема кибершпионажа в международном гуманитарном праве. – *Московский журнал международного права.* № 1. С. 70–80. DOI: https://doi.org/10.24833/0869-0049-2021-1-70-80

Автор заявляет об отсутствии конфликта интересов.

INTERNATIONAL HUMANITARIAN LAW

DOI: https://doi.org/10.24833/0869-0049-2021-1-70-80

Research article
Received 27 December 2020
Approved 14 February 2021

Sergei Yu. GARKUSHA-BOZHKO
School of Higher Sportsmanship in Water Sports named after Yu. S. Tyukalov
10-1, Naberezhnaya Grebnogo kanala, Saint-Petersburg, Russian Federation, 197110
garkusha-bozhko.sergej@yandex.ru
ORCID: 0000-0003-1253-3157

THE PROBLEM OF CYBER ESPIONAGE IN THE INTERNATIONAL HUMANITARIAN LAW

INTRODUCTION. *The article analyses the problem of cyber espionage in the context of armed conflict in cyberspace. The relevance of this research, as part of the problem of international humanitarian law applying in cyberspace, is confirmed by the rapid development of cyber technologies that can be used during armed conflict, as well as the availability of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.*

MATERIALS AND METHODS. *The main sources of this research are the provisions of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, the rules of Additional Protocol I of June 08, 1977 to the Geneva Convention of August 12, 1949, the rules of the Hague Regulations on the Laws and Customs of War on Land of 1907, and the rules of customary international humanitarian law. The methodology consists of the principles used in legal research, as well as general scientific and special methods of legal research (system and formal legal methods).*

RESEARCH RESULTS. *The provisions of the Tallinn Manual on cyber espionage were examined for compliance with the relevant provisions of Additional Protocol I of June 08, 1977 to the Geneva Convention of August 12, 1949, the Hague Regulations on the Laws and Customs of War on Land of 1907, and the rules of customary international humanitarian law, as well as the problems that may arise in the process of possible practical application of this provision of the Tallinn Manual.*

DISCUSSION AND CONCLUSIONS. *It is noted that the provisions of the Tallinn Manual 2.0 on cyber*

espionage are based on the relevant rules of international law. In fact, the relevant provision of the Tallinn Manual is completely copied from the relevant rules of IHL. However, based on the results of this research, the author comes to the conclusion that such blind copying does not take into account the specifics of cyberspace and leads to the following problems in the possible practical application of this provision of the Tallinn Manual: firstly, due to the anonymity of users, it will be difficult to distinguish between a cyber intelligence officer and a cyber spy in practice. Secondly, due to the difficulties in establishing clear state borders in cyberspace, including due to the use of blockchain and VPN technologies, in practice it is impossible to reliably establish whether secret information was collected on the territory of the enemy, which, in turn, leads to difficulties in qualifying such an act as cyber espionage. Finally, in the context of modern armed conflicts, espionage has ceased to be a phenomenon exclusively of international armed conflicts, and therefore it is likely that cyber espionage can be carried out not only in the context of an international armed conflict, but also in the context of a non-international armed conflict. Based on the results of this research, suggestions were made to develop state practice on this issue. It is desirable that States raise the discussion of the above issues at the UN General Assembly, which would help to identify the main trends in the development of such practices. Only And only after the practice of States on this issue becomes more obvious, the question of developing an appropriate international treaty, preferably within the UN, can be raised.

KEYWORDS: *cyber espionage, Computer Network Exploitation, Cyber Reconnaissance, international humanitarian law, armed conflict, Tallinn Manual, espionage, intelligence, cyber spy*

FOR CITATION: Garkusha-Bozhko S.Yu. The Problem of Cyber Espionage in the International Humanitarian Law. – *Moscow Journal of International Law.* 2021. No 1. P. 70–80. DOI: https://doi.org/10.24833/0869-0049-2021-1-70-80

The author declares the absence of conflict of interest.

1. Введение

Развитие информационных технологий в наше время затрагивает все сферы деятельности человечества в мировом масштабе. Не стала исключением и военная деятельность государств. В 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). Иными словами, в современном мире вооруженный конфликт в киберпространстве перестал быть выдумкой писателей-фантастов и сценаристов развлекательных фильмов – теперь это потенциально возможный конфликт, который может начаться из-за столкновения интересов двух и более государств в киберсфере. О вероятности такого конфликта говорится в заявлении российского Президента 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 [Мельцер 2017:51], 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 о вопросе правового регулирования таких конфликтов, 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 Таллинское руководство по международному праву, применимому к кибервооружениям (*Tallinn Manual on the International Law Applicable to Cyber Warfare*).

[1] Путин В. В. Заявление о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности. 25.09. 2020. Доступ: http://kremlin.ru/events/president/news/64086 (дата обращения: 13.12.2020).

Данное 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 этих международно-правовых норм очень высока, что и обусловило принятие новой расширенной версии Руководства в 2017 г. (*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*). Существование Руководства лишний раз доказывает актуальность как проблемы правового регулирования вооруженных конфликтов в киберпространстве, так и проблемы правового регулирования киберпространства в целом.

Конечно, никто не оспаривает тот факт, что в случае начала вооруженного конфликта в киберпространстве к нему будут применяться нормы международного гуманитарного права (МГП). Однако в этой ситуации существует ряд проблем, требующих глубокого исследования. Одна из них – кибершпионаж. Как отмечают исследователи, развитие информационных технологий способствует интересу к правовому исследованию данного явления [Navarrete, Buchan 2019:899]. В настоящей статье мы попробуем разобраться в этой непростой проблеме.

2. Исследование

Норма 89 Таллинского руководства закрепила следующее положение: «Член вооруженных сил, который занимается кибершпионажем на контролируемой противником территории, теряет право быть военнопленным и может рассматриваться как шпион, если он захвачен до возвращения в вооруженные силы, к которым он принадлежит» [Tallinn Manual…2017:409].

Очевидно, что данная норма основана на ст. 29–31 Гаагского «Положения о законах и обычаях сухопутной войны» 1907 г.[2] и на ст. 46 Дополнительного протокола I к Женевским конвенциям 1949 г.[3], которые отражают обычное право [Хенкертс, Досвальд-Бек 2006:497]. Исходя из этих норм, норма о кибершпионаже применима исключительно в международных кибернетических вооруженных конфликтах. Однако отметим, что явление шпионажа сегодня присуще не только международным вооруженным конфликтам.

Практика последних лет показывает, что стороны вооруженного конфликта немеждународного характера также привлекают лиц противной стороны к уголовной ответственности за шпионаж. Это, в частности, подтверждает вооруженный конфликт немеждународного характера на территории юго-востока Украины, в Донбассе. Данный конфликт также имеет особенность – одной из его сторон являются самопровозглашенные государства – Донецкая Народная Республика (ДНР) и Луганская Народная Республика (ЛНР), органы которых и привлекают к ответственности за шпионаж[4].

Так, например, 16 марта 2018 г. Военный трибунал на правах палаты Верховного суда ДНР вынес обвинительный приговор по ст. 321 «Шпионаж» Уголовного кодекса ДНР[5] в отношении Губкиной Ольги Михайловны, гражданки Украины, работавшей на Службу безопасности Украины (СБУ)[6].

Органами МГБ ДНР было установлено, что Губкина О. М. во время ее выезда на территорию Украины в г. Запорожье в результате угроз в ее адрес и психологического давления в виде угроз ее родственникам, постоянно проживающим на территории Украины, со стороны сотрудников УСБУ Запорожской области дала согласие на негласное сотрудничество с указанной службой[7]. Иными словами, она была завербована и стала агентом СБУ. Сотрудничество в данном случае

[2] Документы по международному гуманитарному праву и другие документы, относящиеся к ведению военных действий. М.: МККК. 2012. С. 28-29.

[3] Женевские конвенции от 12 августа 1949 г. и Дополнительные протоколы к ним. М.: МККК. 2011. С. 234–235.

[4] См.: Министерство государственной безопасности ДНР. Официальный сайт. Доступ: http://www.mgbdnr.ru/ (дата обращения: 15.12.2020); Министерство государственной безопасности ЛНР. Официальный сайт. Доступ: http://www.mgblnr.org/ (дата обращения: 15.12.2020).

[5] Уголовный кодекс Донецкой Народной Республики от 19 августа 2014 г. Доступ: https://supcourt-dnr.su/zakonodatelstvo/ugolovnyy-kodeks-doneckoy-narodnoy-respubliki-prinyat-postanovleniem-verhovnogo (дата обращения: 15.12.2020).

[6] Новостная сводка МГБ ДНР. 05.04.2018. Доступ: http://www.mgb-dnr.ru/news.php?id=20180405_00&img_num=0 (дата обращения: 15.12.2020).

[7] Там же.

выразилось в обязанности Губкиной передавать стратегическую информацию, в том числе и секретного характера[8].

Данное дело показывает, что шпионаж в современных условиях перестал быть феноменом исключительно вооруженных конфликтов международного характера, это явление теперь присуще и вооруженным конфликтам немеждународного характера. Особенность рассмотренного дела еще в том, что к ответственности за шпионаж привлекало самопровозглашенное государство в лице своего судебного органа[9] по своему собственному уголовному закону. Более того, аналогичных дел, связанных с вооруженным конфликтом в Донбассе, немало[10], что еще раз подтверждает тезис об эволюции понятия «шпион» в международном гуманитарном праве.

Исходя из этого, полагаем, что и кибершпионаж в современных условиях вряд ли будет явлением исключительно международных кибернетических вооруженных конфликтов – есть вероятность, что действия, попадающие под определение кибершпионажа, будут осуществляться и во время немеждународного кибернетического вооруженного конфликта. Однако не будем сильно критиковать разработчиков Таллинского руководства за ограничение нормы о кибершпионах исключительно международными вооруженными конфликтами в киберпространстве. Данное ограничение обусловлено классическим пониманием шпионажа в МГП. Ограничимся замечанием, что такое классическое понимание не отвечает современным реалиям вооруженных конфликтов.

Далее, в Таллинском руководстве отмечается, что норма о кибершпионах распространяется исключительно на военнослужащих. В случае если кибершпионажем занимается гражданское лицо, такие действия будут актом непосредственного участия в военных действиях, в результате которого гражданское лицо теряет свой иммунитет от нападения и может преследоваться следственными органами воюющего государства [Tallinn Manual…2017:410].

Согласимся с указанным замечанием по следующим причинам. Как известно, под непосредственным участием в военных действиях понимаются «конкретные враждебные акты, совершенные отдельными лицами в рамках ведения военных действий между сторонами в вооруженном конфликте» [Мельцер 2009:52]. Шпионаж, конечно же, является враждебным актом, поэтому полагаем, что такой вид шпионажа в вооруженных конфликтах необходимо считать непосредственным участием гражданских лиц в военных действиях.

Кроме того, практика многих войн, в первую очередь Великой Отечественной войны, подтверждает тезис о том, что участие гражданских лиц в шпионской деятельности представляет собой непосредственное участие в военных действиях, и воюющие государства могут привлекать за это к уголовной ответственности таких лиц. В качестве примера такой практики можно привести уголовное дело арх. № 37932 в отношении И. Ф. Кириллова, М. Ф. Баскакова и И. П. Приемышева, хранящееся в Архиве УФСБ России по г. Санкт-Петербургу и Ленинградской области [Строганов 2009:123].

Дополнительно отметим, что участие гражданских лиц в шпионской деятельности в пользу одного из воюющих государств – не новинка для вооруженных конфликтов. Такие случаи были не только во время Великой Отечественной войны (где к концу 1941 г. уже половина задержанных немецких агентов были гражданами СССР, в том числе и гражданскими лицами [Сизенко 2010:250]), но и во время Первой мировой войны. Достаточно вспомнить Мату Хари, которая была гражданским лицом, но осуществляла шпионскую деятельность в пользу Германии.

Несмотря на выраженное выше согласие с разработчиками Таллинского руководства, отметим, что подход, согласно которому участие гражданских лиц в шпионаже и кибершпионаже признается актом непосредственного участия в военных действиях, является достаточно формальным. Ввиду того, что это достаточно часто встречается на практике и государства привлекают за такие действия к уголовной ответственности, полагаем, что необходимо внести соответствующие изменения в существующие международные договоры по международному

[8] Там же.

[9] О судебной системе. Постановление Совета Министров ДНР № 40-2 от 22 октября 2014 г.. Доступ: https://supcourt-dnr.su/zakonodatelstvo/postanovlenie-soveta-ministrov-doneckoy-narodnoy-respubliki-o-sudebnoy-sisteme-ot (дата обращения: 15.12.2020).

[10] См. сноску 4.

гуманитарному праву в целях предотвращения разночтений существующих норм.

Кибершпионаж в Таллинском руководстве определяется как «любой акт, совершенный тайно или под ложными предлогами, [в процессе осуществления] которого используются кибернетические возможности для сбора (или попытки сбора) информации с намерением передать ее противной стороне» [Tallinn Manual…2017:410]. Подчеркивается, что тайный характер операции кибершпионажа предполагает сокрытие факта ее совершения и личности кибершпиона [Tallinn Manual…2017:410]. Что касается использования ложных предлогов, то оно предполагает создание ложного впечатления, что кибершпион имеет право на доступ к информации, которая является объектом сбора [Tallinn Manual…2017:410].

В свою очередь отметим, что в этом определении чувствуется влияние норм обычного международного гуманитарного права, что неудивительно, т. к. вне зависимости от использования в разведывательной и шпионской деятельности специальных средств, включая информационные технологии, суть такой деятельности (тайный сбор информации) останется неизменной.

Разработчики Таллинского руководства особо подчеркнули, что шпионаж (разведка), включая кибершпионаж, не запрещен правом вооруженных конфликтов и международным правом в целом [Tallinn Manual…2017:410]. На отсутствие такого запрета в международном праве также указывается и в доктрине [Давид 2011:490; Сассоли, Бувье 2008:170; Forcese 2016:72; Tondini 2018-2019:30]. Международное гуманитарное право только закрепляет норму о потере шпионом, который, как известно, скрывает свою принадлежность к вооруженным силам одной из сторон, права быть военнопленным, в отличие от разведчика, который не скрывает своей принадлежности к одной из сторон конфликта (носит ее форму) и сохраняет право на статус военнопленного. Руководство воспроизводит это классическое положение права вооруженных конфликтов [Tallinn Manual…2017:410].

Причины, по которым международное право не запрещает шпионскую деятельность, вполне очевидны. Разведка появилась с момента возникновения первых государств и продолжает существовать как обычное явление в международных отношениях, что подтверждает факт наличия у всех государств разведывательных органов. Государства просто не позволят возникнуть международной норме, запрещающей такую деятельность, т. к. это им невыгодно. Шпионаж запрещен только на уровне национального права государств, что выражено в наличии во всех национальных уголовных законах нормы, предусматривающей уголовную ответственность лиц, занимающихся шпионажем.

Однако в истории с кибершпионажем возникает проблема разграничения шпиона и разведчика, т. к. в силу анонимности пользователей в киберпространстве достоверно установить, является лицо шпионом или разведчиком, невозможно. Поэтому непонятно, почему разработчики Таллинского руководства безапелляционно распространили классическую норму о разграничении и на кибернетические вооруженные конфликты. Очевидно, что норма о разграничении работает в условиях классических вооруженных конфликтов, но в киберпространстве применение данной нормы не будет иметь должного эффекта. По нашему мнению, в отношении данной проблемы разработчики Руководства допустили явную невнимательность.

Интересно замечание Таллинского руководства в отношении географических ограничений данной нормы о кибершпионаже. Ее применение ограничено территорией, контролируемой противником; если деятельность по тайному сбору информации о противнике происходит за пределами указанной территории, то такая деятельность не является кибершпионажем по смыслу данной нормы [Tallinn Manual…2017:411]. Необходимо считать, что такое территориальное ограничение приемлемо для классических вооруженных конфликтов, а в условиях киберпространства данная норма не будет отвечать уровню развития информационных технологий. Так, информационная система, содержащая сведения о противнике, может быть основана на принципах блокчейна (*англ.* – blockchain)[11], т. е. на распределении информации по разным серверам, которые находятся на различных территориях, в том числе не контролируемых противником. Если интересующая шпиона информация нахо-

[11] Более подробно о юридических аспектах блокчейна: Кислый В. А. Юридические аспекты применения блокчейна и использования криптоактивов. – *ЗаконРу.* 05.06.2017. Доступ: https://zakon.ru/blog/2017/6/5/yuridicheskie_aspekty_primeneniya_blokchejna_i_ispolzovaniya_kriptoaktivov (дата обращения: 13.12.2020).

дится на сервере за пределами контролируемой противником территории, то будет ли выгодно противнику исключение такой деятельности по сбору информации из-под действия нормы о кибершпионаже? Представляется, что нет. Поэтому, исходя из того, что границы в киберпространстве достаточно условны, надо полагать, что территориальное ограничение нормы о кибершпионаже, предложенное Таллинским руководством, не отвечает реалиям вооруженных конфликтов в киберпространстве.

Странным также выглядит комментарий Руководства о характере собираемой в ходе кибершпионажа информации. Большинство членов Международной группы экспертов пришли к выводу, что ее характер не имеет значения, и только лишь малая часть экспертов отметила, что собираемая информация должна представлять определенную военную ценность [Tallinn Manual…2017:412]. Естественно, что в ходе вооруженного конфликта, в том числе и кибернетического, сторонам конфликта будет интересна именно информация военного характера, и на практике шпионы собирают именно информацию военного характера, в том числе и в киберпространстве. Поэтому непонятно, почему разработчики Таллинского руководства не учли этот очевидный факт.

Интересно также отметить, что в Таллинском руководстве есть положения о кибершпионаже в мирное время. В целях проведения более полного исследования считаем важным изучить и этот вопрос, т. к. он тесно связан и с вопросом кибершпионажа в контексте международного гуманитарного права.

Норма 32 Руководства закрепила следующие положения: «Хотя кибершпионаж, [осуществляемый] в мирное время государствами, сам по себе не нарушает международное право, метод, путем которого он осуществляется, может допустить это [нарушение]» [Tallinn Manual…2017:168]. Применительно к данной норме под кибершпионажем понимается любой акт, предпринятый тайно или под ложными предлогами, [в ходе] которого используются кибервозможности для сбора или попытки сбора информации [Tallinn Manual …2017:168]. Кроме того, кибершпионаж включает, но не ограничивается, использованием кибервозможностей для наблюдения, мониторинга, захвата или вывода электронно передаваемых или хранимых сообщений, данных или другой информации [Tallinn Manual…2017:168]. Надо полагать, что такое широкое толкование действий, квалифицируемых в качестве акта кибершпионажа, распространяется не только на мирное время, но и на военное, т. к. стороны вооруженного конфликта тоже заинтересованы в таких действиях.

Однако странным выглядит замечание разработчиков Таллинского руководства о том, что указанное определение используется только для целей нормы 32 и не имеет самостоятельного правового значения. По нашему мнению, в силу отсутствия международно-правового определения шпионажа предложенное Руководством определение представляет интерес не только с точки зрения доктринального исследования, но и для дальнейшей разработки соответствующей нормы международного права.

Пункт 3 комментария к норме 32 содержит очень важное замечание, что кибершпионаж ограничивается действиями, которые присваиваются исключительно только государствам [Tallinn Manual…2017:168]. Данное замечание обусловлено очевидным фактом, что шпионаж – это явление межгосударственных отношений с момента появления первых государств, и новый вид шпионажа – кибершпионаж – не исключение. Что касается так называемого коммерческого шпионажа, осуществляемого одной коммерческой компанией против другой, то это явление сугубо частных коммерческих отношений, и поэтому выходит за рамки настоящей работы.

Таллинское руководство делает не менее важное замечание, что кибершпионаж имеет ряд преимуществ перед традиционными методами шпионажа. В частности, в качестве преимуществ кибершпионажа отмечены скорость получения информации и ее объемы [Tallinn Manual… 2017:168]. Но самым главным преимуществом кибершпионажа является возможность удаленного доступа к интересующим информационным системам без физического присутствия в государстве-жертве. Так, сотрудник Центрального разведывательного управления США (ЦРУ, *Central Intelligence Agency, CIA*), находясь в штабквартире данного разведывательного органа в Лэнгли, округ Фэрфакс, штат Виргиния, всего лишь в 13 км от столицы США, может с помощью использования информационных технологий получить доступ к информационной системе правительства какого-нибудь государства европейского континента. В наши дни такие возможности уже стали обычным делом для разведок мира, на что и обращает внимание Таллиннское руководство [Tallinn Manual…2017:168].

Кроме того, как указывают в Руководстве [Tallinn Manual…2017:168-169], каждый из трех уровней киберпространства может способствовать кибершпионажу. В рамках физического уровня можно изначально так запрограммировать оборудование, чтобы в дальнейшем заинтересованное в получении информации государство получило удаленный доступ к ней, либо так проложить пути передачи информации, чтобы была возможность тайного перехвата данных.

В рамках логического уровня действенным методом кибершпионажа будет использование различного вредоносного программного обеспечения. И, наконец, в рамках социального уровня наиболее действенны методы социальной инженерии, самым известным из которых является фишинг. Иными словами, доступ к заветной информационной системе производится путем обманного завладения учетными данными пользователей, что обеспечивает шпионам вход в такую информационную систему.

Таким образом, благодаря современным технологиям разведывательная и шпионская деятельность настолько изменились, что можно получить информацию об интересующем государстве, находясь за тысячи километров от него. И еще раз подчеркнем, что по общему правилу такая деятельность не запрещена международным правом. Однако если определенные методы кибершпионажа нарушают нормы международного права, в частности, принцип невмешательства во внутренние дела государства, суверенитет государства и права человека, то такие действия в киберпространстве однозначно будут являться международно-противоправными деяниями. Это особо подчеркивается и в Таллинском руководстве [Tallinn Manual…2017:170].

Анализируя предложения Таллинского руководства о кибершпионаже в целом, необходимо согласиться с мнением, выраженным в доктрине [Navarrete 2015:10], что Руководство предлагает «оперативное» определение, разработанное на основе ст. 29 Гаагского положения. Эта «оперативность» выражается в том, что кибершпионская деятельность осуществляется тайно или под ложными предлогами. Но, помимо этого «оперативного» критерия, в определении кибершпионажа в рамках вооруженного конфликта также содержится персональный критерий, который характеризует исполнителя такой деятельности.

Важно также отметить, что Таллинское руководство, помимо кибершпионажа, выделяет еще два близких ему вида деятельности. Это, во-первых, эксплуатация компьютерных сетей (*Computer Network Exploitation, CNE*), а, во-вторых, киберразведка (*Cyber Reconnaissance*). Указанные виды кибердеятельности отличаются от кибершпионажа тем, что они осуществляются за пределами территории, контролируемой противником [Tallinn Manual…2017:335, 564].

Конечно, причины такого разграничения вполне понятны. Однако, по нашему мнению, исходя из того, что на практике государства расценивают любую иностранную деятельность по тайному сбору информации о них как акты шпионажа, такое различие будет существовать исключительно на бумаге, а не на практике. Здесь уместно вспомнить, что для государства сотрудники его разведывательных органов всегда будут разведчиками, а сотрудники иностранных разведывательных органов всегда будут шпионами. Поэтому еще раз подчеркнем, что данное различие, предложенное Руководством, является относительным. Однако в доктрине не обращают внимания на относительность данного разграничения [Yoo 2015:12, 26; Navarrete 2015:10-11].

Затрагивая территориальный критерий, необходимо вспомнить типологию шпионажа, предложенную Крейгом Форсезе. Согласно этой точке зрения можно выделить территориальный шпионаж, экстратерриториальный шпионаж и транснациональный шпионаж [Forcese 2011:183-184]. Кибершпионаж относится к последнему типу – транснациональному, когда территориальная привязка играет наименьшую роль, поэтому, исходя из этого, не совсем ясно, как на практике разграничить кибершпионаж, эксплуатацию компьютерных сетей и киберразведку. Проблемы в данном разграничении возникнут также по мере более широкого распространения технологии *VPN*, позволяющей маскировать настоящий *IP*-адрес. Поэтому не понятно, как в условиях использования данной технологии точно установить местоположение кибершпиона. Очевидно, что, закрепив разграничение между вышеуказанными понятиями, разработчики Таллинского руководства не учли сложности при определении действительного местонахождения кибершпиона и возможности технологии *VPN*, тем самым допустив огромное упущение.

В этой связи уместно будет согласиться с авторами, которые отмечают, что концепции эксплуатации компьютерных сетей и киберразведки являются сугубо доктринальными [Navarrete 2015:22]. В свою очередь, добавим, что на практике это разграничение, предложенное Тал-

линским руководством, скорее всего, потерпит фиаско и государства будут квалифицировать большинство актов по тайному сбору информации в киберпространстве как кибершпионаж. С учетом вышеуказанной условности различия между разведкой и шпионажем необходимо использовать только термин «кибершпионаж» во избежание разночтений.

Кроме того, практика мирного времени подтверждает, что акты по тайному сбору информации в киберпространстве чаще всего квалифицируются как кибершпионаж. В подтверждение этого можно привести историю с китайской шпионской киберсетью *GhostNet*, в результате деятельности которой были взломаны не менее 1295 информационных систем в 103 государствах мира [Kerschischnig 2012:171]. В частности, 30 % таких информационных систем находились в правительственных структурах различных государств: по 11 – в Министерстве иностранных дел Бутана и в посольстве Мальты в Бельгии и семь – в посольстве Индии в США [Kerschischnig 2012:171]. Были взломаны также восемь информационных систем в офисе крупнейшего оператора связи Венесуэлы; три – в офисах Азиатского банка развития и более 150 компьютеров – в штаб-квартирах торговых союзов Вьетнама и Тайваня [Kerschischnig 2012:171]. По одной взломанной информационной системе было обнаружено в посольствах Португалии, Румынии, Кипра, Индии, Таиланда, Германии, расположенных в разных странах мира, и в штабе Верховного главнокомандующего Объединенными вооруженными силами НАТО в Европе [Kerschischnig 2012:171]. Также десятки информационных систем были взломаны в организациях, борющихся за независимость Тибета: в резиденциях Его Святейшества Далай-ламы и тибетского правительства в изгнании, в штаб-квартирах различных протибетских организаций в Нью-Йорке, Лондоне, Брюсселе и Женеве [Kerschischnig 2012:171; Moore 2010:5].

Еще из примеров шпионских программных обеспечений можно отметить программное обеспечение троянского типа под названием *Flame*, которое использовалось для шпионажа в Иране, Ливане, Сирии, Судане, Израиле и Палестине [Woltag 2014:41][12]. Как сообщила российская компания «Лаборатория Касперского», *Flame* по сложности и функционалу превосходит *Duqu* и *Stuxnet*[13].

Вышеуказанные примеры были квалифицированы как шпионское программное обеспечение. Иными словами, это примеры кибершпионажа. Надо полагать, что вряд ли государства, в информационные сети которых будут вмешиваться с целью сбора информации, будут квалифицировать такие действия как-то иначе.

В контексте территориальности не менее важно напомнить, что государственные границы в киберпространстве условны и установить четкие границы суверенитета отдельного государства достаточно сложно. В настоящий момент практика государств не позволяет сделать однозначные выводы в отношении границы суверенитета государства в киберпространстве. На это указывают и в доктрине [Lafouasse 2012:161; Bourguignon 2014:362, 396; Navarrete 2015:22-23]. Данный факт также усложняет вопрос о разграничении кибершпионажа от смежных действий.

В заключение рассуждений о территориальном критерии кибер-шпионажа, хотелось бы привести позицию Министерства обороны США: «Несанкционированное электронное вторжение в компьютерные системы другого государства вполне может быть расценено как нарушение суверенитета жертвы. Это может даже рассматриваться как равносильное физическому вторжению на территорию государства, но такие вопросы еще предстоит решить в международном сообществе» [Peacetime Regime…2013:458]. В контексте данного утверждения очевидно, что государства чувствительно относятся к вторжению в их информационные системы. В свете этого вывод о сложности проведения различия между кибершпионажем, эксплуатацией компьютерных сетей и киберразведкой на практике лишний раз подтверждается.

Нет оснований полагать, что вышеуказанные размышления не применимы к кибершпионажу в контексте вооруженного конфликта. Выше обозначенные проблемы также могут возникнуть и в случае вооруженного конфликта.

[12] Eudes Yv. Flame, un virus espion d'Etat. – *Le Monde*. 20.06. 2012. URL: https://www.lemonde.fr/technologies/article/2012/06/20/flame-un-virus-espion-d-etat_1721182_651865.html (accessed 15.12.2020).

[13] Ализар А. Flame/Flamer/sKyWiper: сложнейший троян для таргетированного шпионажа в Иране. 29.05.2012. Доступ: https://xakep.ru/2012/05/29/58762/ (дата обращения: 15.12.2020).

3. Заключение

Таким образом, на основании проведенного анализа можно сделать следующий вывод. Норма Таллинского руководства о кибершпионаже по сути является слепым копированием классической нормы МГП о шпионаже, не учитывающей возможных проблем, которые могут возникнуть в киберпространстве. В частности, во-первых, в силу анонимности пользователей на практике будет сложно провести разграничение между киберразведчиком и кибершпионом.

Во-вторых, в силу сложностей в установлении четких государственных границ (установлении границ государственного суверенитета) в киберпространстве, в том числе, обусловленных использованием технологий блокчейн и VPN, на практике невозможно достоверно установить, осуществлялся ли тайный сбор информации на территории противника, что, в свою очередь, влечет сложности в квалификации такого деяния в качестве кибершпионажа.

И, наконец, необходимо отметить, что в условиях современных вооруженных конфликтов шпионаж перестал быть явлением исключительно международных вооруженных конфликтов, и поэтому есть вероятность, что кибершпионаж может осуществляться не только в контексте вооруженного конфликта международного характера, но и в контексте вооруженного конфликта немеждународного характера.

Конечно, можно бесконечно критиковать разработчиков Таллинского руководства по поводу упущения из внимания вышеуказанных проблем. Однако мы не будем этого делать, так как понимаем, что необходимо учитывать, что практика государств в отношении данного вопроса в полной мере еще не сформирована, и поэтому рано делать какие-либо окончательные выводы. Для начала необходимо, чтобы государства сформировали соответствующую практику. Желательно, чтобы государства подняли обсуждение вышеуказанных проблем на Генеральной Ассамблее ООН, что помогло бы выделить основные тренды развития такой практики. И только после того, как практика государств по данному вопросу станет более очевидной, можно ставить вопрос о разработке соответствующего международного договора, желательно на площадке ООН.

Список литературы

1. Давид Э. 2011. *Принципы права вооруженных конфликтов: курс лекций, прочитанных на юридическом факультете Открытого Брюссельского университета.* М.: МККК. 1444 с.
2. Мельцер Н. 2017. *Международное гуманитарное право: общий курс.* М.: МККК. 420 с.
3. Мельцер Н. 2009. *Непосредственное участие в военных действиях: руководство по толкованию понятия в свете международного гуманитарного права.* М.: МККК. 107 с.
4. Сассоли М., Бувье А. 2008. *Правовая защита во время войны. Том I.* М.: МККК. 672 с.
5. Сизенко А. Г. 2010. *Спецслужбы России и СССР: от Приказа тайных дел до наших дней.* Ростов-на-Дону.: Издательский дом «Владис». 416 с.
6. Строганов П. П. 2009. *Щит и меч блокадного Ленинграда.* СПб.: Агентство ВиТ-принт. 295 с.
7. Хенкертс Ж.-М., Досвальд-Бек Л. 2006. *Обычное международное гуманитарное право. Том I. Нормы.* М.: МККК. 819 с.
8. Bourguignon J. 2014. La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'Etat. – *Société Française pour le droit International – Colloque. Internet et le droit international.* Paris: Éditions A. Pedone. P. 357–372.
9. Forcese C. 2016. Pragmatism and Principle: Intelligence Agencies and International Law. – *Virginia Law Review Online.* Vol. 102. P. 67–84
10. Forcese C. 2011. Spies Without Borders: International Law and Intelligence Collection. – *Journal of National Security Law & Policy*. Vol. 5. P. 179–210.
11. Kerschischnig G. 2012. *Cyberthreats and International Law.* The Hague: Eleven international publishing. 386 p.
12. Lafouasse F. 2012. *L'Espionnage dans le droit international.* Paris.: Nouveau Monde. 500 p.
13. Moore T. 2010. Introducing the Economics of Cybersecurity: Principles and Policy Options. – *National Research Council, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington, D. C.: The National Academies Press. P. 3–23.
14. Navarrete I., Buchan R. 2019. Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions. – *Cornell International Law Journal.* Vol. 51. Issue 4. P. 897–954.
15. Navarrete I. 2015. L'espionnage en temps de paix en droit international public. – *Canadian Yearbook of International Law.* Vol. 53. P. 1–65.
16. *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy.* Ed. by K. Ziolkowski. 2013. Tallinn: NATO CCD COE. 746 p.
17. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Ed by L. Vihul. 2017. Cambridge: Cambridge University Press. 598 p.
18. Tondini M. 2018-2019. Espionage and International Law in the Age of Permanent Competition. – *Military Law and Law of War Review.* Vol. 57. Issue 1. P. 17–58.

19. Yoo Ch. S. 2015. Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures. – *University of Pennsylvania Carey Law School Scholarship.* No. 1540. 32 p. URL: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2541&context=faculty_scholarship (дата обращения 27.11.2020).
20. Woltag J.-Ch. 2014. *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law.* Cambridge: Intersentia. 314 p.

References

1. Bourguignon J. La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'Etat. – *Société Française pour le droit International – Colloque. Internet et le droit international.* Paris: Éditions A. Pedone. 2014. P. 357–372.
2. David E. Principes de droit des conflits armés: précis de la faculté de droit de l'universite libre de Bruxelles (Russ. ed.: David E. *Printsipy prava vooruzhennykh konfliktov: kurs lektsii, prochitannykh na yuridicheskom fakul'tete Otkrytogo Bryussel'skogo universiteta.* Moscow: MKKK Publ. 2011. 1144 p.)
3. Forcese C. Pragmatism and Principle: Intelligence Agencies and International Law. – *Virginia Law Review Online.* 2016. Vol. 102. P. 67–84.
4. Forcese C. Spies Without Borders: International Law and Intelligence Collection. – *Journal of National Security Law & Policy.* 2011. Vol. 5. P. 179–210.
5. Henckaerts J.-M., Doswald-Beck L. Customary International Humanitarian Law. Volume I: Rules (Russ. ed.: Henckaerts J.-M., Doswald-Beck L. *Obychnoe mezhdunarodnoe gumanitarnoe pravo. Tom I. Normy.* Moscow: MKKK Publ. 2006. 819 p.)
6. Kerschischnig G. *Cyberthreats and International Law.* The Hague: Eleven international publishing. 2012. 386 p.
7. Lafouasse F. *L'Espionnage dans le droit international.* Paris.: Nouveau Monde. 2012. 500 p.
8. Melzer N. International Humanitarian Law. A Comprehensive Introduction (Russ. ed.: Melzer N. *Mezhdunarodnoe gumanitarnoe pravo: obshchii kurs.* Moscow: MKKK Publ. 2017. 420 p.)
9. Melzer N. Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law (Russ. ed.: Melzer N. *Neposredstvennoe uchastie v voennykh deistviyakh: rukovodstvo po tolkovaniyu ponyatiya v svete mezhdunarodnogo gumanitarnogo prava.* Moscow: MKKK Publ. 2009. 107 p.)
10. Moore T. Introducing the Economics of Cybersecurity: Principles and Policy Options. – *National Research Council, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington, D. C.: The National Academies Press. 2010. P. 3–23.
11. Navarrete I. L'espionnage en temps de paix en droit international public. – *Canadian Yearbook of International Law.* 2015. Vol. 53. P. 1–65.
12. Navarrete I., Buchan R. Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions. – *Cornell International Law Journal.* 2019. Vol. 51. Issue 4. P. 897–954.
13. *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy.* Ed. by K. Ziolkowski. Tallinn: NATO CCD COE. 2013. 746 p.
14. Sassoli M., Bouvier A. How does Law protect in war? Vol. 1 (Russ. Ed.: Sassoli M., Bouvier A. *Pravovaya zashchita vo vremya voiny. Tom I.* Moscow: MKKK Publ. 2008. 672 p.)
15. Sizenko A. G. *Spetssluzhby Rossii i SSSR: ot Prikaza tainykh del do nashikh dnei* [Special services of Russia and the USSR: from the Order of secret affairs to the present day]. Rostov-on-Don: Izdatel'skii dom "Vladis" Publ. 2010. 416 p. (In Russ.)
16. Stroganov P. P. *Shchit i mech blokadnogo Leningrada* [Shield and sword of besieged Leningrad]. Saint-Petersburg: Agentstvo ViT-print Publ. 2009. 295 p. (In Russ.)
17. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Ed by L. Vihul. Cambridge: Cambridge University Press. 2017. 598 p.
18. Tondini M. Espionage and International Law in the Age of Permanent Competition. – *Military Law and Law of War Review.* 2018-2019. Vol. 57. Issue 1. P. 17–58.
19. Woltag J.-Ch. *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law.* Cambridge: Intersentia. 2014. 314 p.
20. Yoo Ch. S. Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures. – *University of Pennsylvania Carey Law School Scholarship.* 2015. No. 1540. 32 p. URL: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2541&context=faculty_scholarship (accessed 27.11.2020).

Информация об авторе

Сергей Юльевич Гаркуша-Божко,
юрисконсульт, Школа высшего спортивного мастерства по водным видам спорта имени Ю.С. Тюкалова

197110, Российская Федерация, Санкт-Петербург, наб. Гребного канала, д. 10, стр. 1

garkusha-bozhko.sergej@yandex.ru
ORCID: 0000-0003-1253-3157

About the Author

Sergei Yu. Garkusha-Bozhko,
Legal Counsel, School of Higher Sportsmanship in Water Sports named after Yu. S. Tyukalov

10-1, Naberezhnaya Grebnogo kanala, Saint-Petersburg, Russian Federation, 197110

garkusha-bozhko.sergej@yandex.ru
ORCID: 0000-0003-1253-3157