УДК 341.3

Петрова Антонина Сергеевна
Санкт-Петербургский государственный университет
Юридический факультет
Россия, Санкт-Петербург
ant.petrova13@gmail.com
Petrova Antonina
St. Petersburg University
Faculty of Law
Russia, St. Petersburg

КИБЕРАТАКА И ИНТЕРНЕТ-ВИРУСЫ: ОБЛАСТЬ ПРИМЕНЕНИЯ ЖЕНЕВСКИХ КОНВЕНЦИЙ

Аннотация: в настоящей статье автор поднимает проблему применения норм права к кибернападениям и Интернет-вирусам. Последовательно определяя, что такое кибератака и Интернет-вирус, автор приходит к выводу о применении Женевских конвенций к данным средствам ведения войны. Кибернападение должно быть пропорциональным и избирательным, для того чтобы его возможно было счесть правомерным. Вместе с тем, использование Интернет-вируса как средства ведения войны и осуществления нападения может быть признано неизбирательным и неправомерным, в зависимости от целей его распространения.

Ключевые слова: кибернападение, комбатанты, виды оружия, Интернет-вирусы, международное гуманитарное право, Женевские конвенции.

CYBERATTACK AND INTERNET VIRUSES: THE SCOPE OF APPLICATION OF THE GENEVA CONVENTIONS

Annotation: in this article the author raises the problem of application of law to cyberattacks and Internet viruses. Consistently defining what a cyberattack and an Internet virus are, the author concludes on the application of the Geneva Conventions to these means of warfare. Cyber-attacks must be proportional and selective in order to be considered legitimate. However, the use of an Internet virus as a means of warfare and attack may be considered indiscriminate and unlawful, depending on the purpose of its dissemination.

Key words: cyberattack, combatants, types of weapons, Internet viruses, international humanitarian law, Geneva Conventions.

Современный мир и компьютерные технологии, а также всемирная сеть Интернет сегодня всецело взаимосвязаны. Именно поэтому вопросы права, применимые к физическому миру, становятся применимы к миру виртуальному. Право в сети «Интернет» весьма обширно, к нему относятся нормы гражданского права, уголовного, а также международного. Говоря о международном праве нельзя не сказать о праве гуманитарном и праве вооруженных конфликтов. Данные отрасли в области предмета своего регулирования также применимы к отношениям, возникающим в кибер- и Интернет-пространстве.

Какими бы мирными ни были цели создания глобальной сети, к сожалению, она используется в том числе в военных целях. Вместе с тем, чтобы не допустить произвола и нарушений права человека, необходимо правовое регулирование использования киберпространства в вооруженных конфликтах. Как отмечают в доктрине [4], киберпространство является «пятой сферой или пятым доменом ведения военных действий» после суши, моря, воздушного и космического пространств.

Право вооруженных конфликтов, основу которого составляют Женевские конвенции 1949 года (а также Гаагские конвенции 1899 и 1907 годов и ряд

других международных договоров, включая Санкт-Петербургскую декларацию 1868 года), разрабатывалось задолго до возникновения киберпространства. В этой связи данные международные договоры предусматривали последствия ведения физической войны. Однако случаи кибератаки, заражения сетей Интернет-вирусами становятся все более частыми.

Смоделировать ситуации, в которых кибератаки затрагивали гражданское население, можно множество. В связи с ними возникают вопросы правовой квалификации, как во время вооруженных конфликтов, так и в мирные годы. К примеру, проведение кибероперации, направленной на остановку или сбой нормального функционирования энергетической системы или системы водоснабжения, использующихся в гражданских целях, без их физической ликвидации [1].

Вспомним пример компьютерного вируса Stuxnet, созданного для остановки функционирования завода по обогащению урана в городе Нетензе (Иран). Этот случай – показательный пример длительного враждебного воздействия на государственные информационные системы [6].

Некоторые эксперты утверждают [3], что вирус Stuxnet – яркий пример кибератаки. Его внедрение осуществлено в нарушение основополагающего принципа международного права неприменения силы и угрозы ею, а также в нарушение норм *jus in bello*.

Было установлено, что вирус был разработан при участии специалистов из спецслужб Израиля и США. Целью поражения стала ядерная программа Ирана. С одной стороны, данный вирус был направлен не на гражданский объект (по квалификации Дополнительного протокола I к Женевским конвенциям). Кроме того, ядерная программа не была физически уничтожена: воздействие оказано исключительно на информационные системы. Однако воздействие этого вируса объективно носило характер нападения.

Для ответа на вопрос о применимом праве, необходимо разобраться в понятии кибератака и Интернет-вируса.

Кибератака совершается *a priori* в киберпространстве (или в информационном пространстве). В статье 2 Конвенции об обеспечении международной информационной безопасности, вынесенной Российской Федерацией в 2011 г. на рассмотрение в Организацию Объединенных Наций (ООН), информационное пространство понимается как 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 [7].

Аналогичный подход воспринят в Соглашениях Правительств Российской Федерации с Правительствами Республики Беларусь [8] и Китайской Народной Республики [9].

Однако Интернет и киберпространство не одно и то же. Интернет входит в киберпространство, но последнее не ограничивается им. В Доктрине информационной безопасности Российской Федерации киберпространство определено как совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений [10]. Примечательно, что киберпространство как термин в Доктрине не используется, для обозначения этого явления применяется понятие «информационная сфера».

Итак, кибератака возможна не только в сети «Интернет», но на сети связи, иные сети, связанные с безопасностью государства или субъекта государства. Кибернападение осуществляется только в условиях вооруженного конфликта в киберпространстве. Вооруженный конфликт в киберпространстве, по смыслу Таллинского руководства 2017 года, имеет место, когда между двумя и более государствами происходят военные действия с использованием кибероперациий и иных киберсредств (нормы 80-83) [6].

Кибератака – разновидность кибероперации. Таллинское руководство в норме 92 [6] дает легальную дефиницию данному термину. Кибератака – это наступательная или оборонительная кибероперация, которая, как разумно ожидается, приведет к причинению травм или смерти людей, либо к повреждению или разрушению объектов [6].

Российское законодательство также содержит понятие компьютерной атаки в статье 2 Федерального закона №187-ФЗ: «компьютерная атака — целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации» [11].

Таким образом, кибернападение своей целью имеет причинение имущественного ущерба противнику и его человеческим ресурсам. Оно может быть как в сети «Интернет», так и за его пределами. Попадает ли такое нападение под регулирование права вооруженных конфликтов?

На наш взгляд, да, попадает. Кибератака должна регулироваться нормами Женевских конвенций в полной мере. Данное умозаключение следует, во-первых, из общего понятия нападения, закрепленное статьей 49 Дополнительного протокола I к Женевским конвенциям. Во-вторых, из статьи 36 Дополнительного протокола I, которая обязует страны использовать новые

виды оружия в соответствии с нормами международного права. Средства осуществления кибернападений на сегодняшний день не урегулированы международным правом, однако международное гуманитарное право распространяется на них.

Теперь остановимся подробнее на сфере применения норм МГП к кибернападениям. Поднимем три вопроса: (1) различие между комбатантами и не комбатантами; (2) различие между гражданской и военной инфраструктурой; и (3) принцип пропорциональности.

Во-первых, при квалификации киберпреступников или кибернападающих (осуществляющих фактические действия для проведения операции в киберпространстве) как комбатантов или не комбатантов, то они лишаются статуса комбатанта, поскольку они не идентифицируют себя ними. Согласно Гаагским конвенциям, статусом комбатанта обладают только военнослужащие регулярных вооруженных сил страны, которые имеют право применять силу к законным военным целям. Комбатанты должны соблюдать нормы международного права, применяемого в период вооруженных конфликтов, хотя их несоблюдение не лишает их статуса комбатанта. Согласно ст. 44 Дополнительного протокола I к Женевским конвенциям [12], комбатант обязан себя отличать от гражданского населения, носить открыто оружие и форму, идентифицирующую его как комбатанта. Лицо, осуществляющее действие фактического кибернападения может не состоять в вооруженных силах государства, оно может не идентифицировать себя как комбатанта. Лицом, следующим за регулярной армией или иным персоналом, исполнитель кибератаки также не является. Вопрос статуса киберпреступников остается дискуссионным. Если такие лица состоят в вооруженных силах, то они a priori будут являться комбатантами. Вероятно, в каждом отдельном случае необходимо применять нормы международного гуманитарного права исходя из фактической ситуации и действий кибератакующего.

Во-вторых, кибератаки превышают ограничения МГП на допустимые цели. Женевское право проводит различие между военными и гражданскими лицами, объектами, ограничивают пределы нападения военными объектами. Статья 52(2) Дополнительного Протокола I гласит [12], что «военные объекты ограничиваются теми объектами, которые в силу своего характера, расположения, назначения или использования вносят эффективный вклад в военные действия и полное или частичное разрушение, захват или нейтрализация которых при существующих в данный момент обстоятельствах дает явное военное преимущество». Другими словами, инфраструктура, не вносящая прямого вклада в военные действия, остается недоступной для преднамеренного нападения. Полагаем, что нападение в области киберпространства также должно иметь целью поражения исключительно военные объекты. В ином случае, применение силы будет непропорциональным, принесет излишние страдания гражданскому населению. Учитывая, что кибератаки зачастую могут выходить из-под контроля, особенно с применением Интернет-вирусов, цель которых общее распространение, то к применению данного принципа международного гуманитарного следует подходить особенно внимательно.

В-третьих, большая часть ответственности за сопутствующий ущерб в результате непропорциональных атак возлагается на обороняющиеся силы, которые не смогли должным образом изолировать и защитить гражданские объекты. Ст. 51 Дополнительного протокола I гласит [12]: «нападение, которое, как можно ожидать, попутно повлечет за собой потери жизни среди гражданского населения, ранения гражданских лиц и ущерб гражданским объектам или то и другое вместе, которые были бы чрезмерны по отношению к конкретному и непосредственному военному преимуществу, которое предполагается таким образом получить». Этот принцип подразумевает установление баланса между военным преимуществом и возможным ущербом

гражданскому населению. Применительно к кибератакам, отметим, что гражданскими объектами могут быть любые сети, которые не используются в военных целях: от социальных сетей в Интернете до средств обеспечения электроэнергией больниц.

В совокупности, рассмотренные выше положения международного гуманитарного права указывают на то, что в существующих нормах нет прямого запрета на кибератаки, они, как и нападения физические, должны соответствовать принципам пропорциональности, избирательность и соразмерности.

Интернет-вирус – это новый вид оружия? Интернет-вирус – это вредоносная программа, способная внедряться в коды иных программ, сектора загрузки, а также распространять свои копии. Цель вируса как такового – распространение. В его функции входят удалений файлов, удаление операционной системы, нарушение работоспособности сетевых структур, кража персональных данных и многие другие. Вирус может быть распространен не только через сеть Интернет, но и через внешние носители. Примечательно, что вирусами в обывательском смысле называют все вредоносное программы. Тем не менее, использование собственно вирусов с помощью сети «Интернет» можно квалифицировать как кибероружие, если он соответствует определенным критериям.

В случае если такой вирус используется для осуществления превентивного удара, дезорганизации командования, диверсии, иного вида наступления, характеризуется глобальной досягаемостью, мгновенным воздействием [2], имеет целью уничтожение и нарушения объектов, то его можно классифицировать в качестве кибероружия.

Особенностью вирусов, находящихся в файлах и распространенных в сети «Интернет», является то, что они доступны максимально широкому кругу лиц и, в первую очередь, они доступны лицам гражданским. То есть принцип

избирательности при осуществлении нападения с помощью такого кибероружия как Интернет-вирус соблюсти чрезвычайно трудно. Следовательно, распространение такого вируса и уничтожение персональных файлов, кража персональных данных гражданских лиц, а также блокировка работы объектов из жизненно важных отраслей, будут признаны неизбирательным нападением, причиняющим излишние страдания. Следовательно, такое нападение будет неправомерным, противоречащим нормам международного права.

В таком случае, государство, допустившее или разрешившее распространение такого Интернет-вируса, может быть ответственно в соответствии с нормами международного права.

Таким образом, при распространении в сети «Интернет» вредоносных программ и вирусов с целью совершения нападения на определенное государство попадает под действие норм международного гуманитарного права. Вместе с тем, важным вопросом является классификация такого нападения. В случае если распространение вируса направлено на уничтожение гражданских объектов, причинение страданий гражданским лицам (через уничтожение серверов, кражи персональных данных и иным образом), то такое нападение будет неизбирательным и непропорциональным.

Список литературы:

1. Гаркуша-Божко С. Ю. Международное гуманитарное право в киберпространстве: Ratione materiae, ratione temporis и проблема квалификации кибератак. // Цифровое право. – 2021. – №2(1). – С. 64–82.

2. Каберник В. В. Проблемы классификации кибероружия. // Вестник МГИМО. – 2013. – №2(29). – С. 72-78.

3. Brown G. D. Why Iran didn’t admit Stuxnet was an attack. // Joint Force Quarterly. – 2011. – № 63. – P. 70–73.

4. Melzer N. Cyber War and International Law United Nations Institute for Disarmament Research Resources. [Электронный ресурс] // URL: https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf

5. Schmitt M.N. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. // Harvard International Law Journal. – 2012. – P. 13-37.

6. Schmitt, M. N. (Ed.). Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. [Электронный ресурс] // URL: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

7. МИД России. (2011, сентябрь 22). Конвенция об обеспечении международной информационной безопасности (концепция). [Электронный ресурс]//URL:https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

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

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

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

11. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

12. Дополнительный протокол I к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов от 8 июня 1977 года // СПС «КонсультантПлюс».