Научная статья
УДК 341.3
DOI 10.33184/pravgos-2024.3.18

ХОДАНОВ Андрей Иванович
Российская таможенная академия,
Москва, Россия,
e-mail: ai.hodanov@customs-academy.ru,
https://orcid.org/0009-0003-6166-1128

Original article

KHODANOV Andrei Ivanovich
Russian Customs Academy, Moscow, Russia.

ПРОБЛЕМЫ ПРИДАНИЯ СТАТУСА CASUS BELLI КИБЕРАТАКЕ НА ГОСУДАРСТВО – ЧЛЕНА НАТО

CHALLENGES OF GRANTING THE STATUS OF CASUS BELLI TO A CYBERATTACK ON A NATO MEMBER STATE

Аннотация. *В статье анализируются проблемы, связанные с признанием кибератаки на государство – члена НАТО поводом для объявления войны (casus belli). Раскрыта эволюция подходов Североатлантического союза к вопросам киберугроз и киберзащиты, начиная с Пражского саммита 2002 г. и заканчивая Брюссельским саммитом 2021 г. Рассмотрены критерии, предложенные в Таллиннском руководстве по международному праву, применимому при ведении кибервойны, которые позволяют отнести кибератаку к акту применения силы. Приведены статистические данные о кибератаках и отмечена их значимость для международного права и кибербезопасности. Цель: анализ условий и обстоятельств, при которых кибератака может считаться странами НАТО поводом для объявления войны. Методы: формально-юридический, историко-системный, ретроспективный. Выводы: во-первых, несмотря на существующие международные правовые нормы, критерии для признания кибератаки casus belli остаются нечеткими, что позволяет странам НАТО сохранять гибкость в реагировании на киберугрозы; во-вторых, применение странами НАТО ст. 5 Североатлантического договора не обязывает в безусловном и безальтернативном порядке начать вооруженные действия против государства – источника атаки, а лишь требует от других членов НАТО оказать любую возможную и надлежащую помощь пострадавшей стороне.*

Ключевые слова: *casus belli, кибератака, кибероперация, международное право, НАТО, саммиты, Таллиннское руководство*

Для цитирования: Ходанов А.И. Проблемы придания статуса casus belli кибератаке на государство – члена НАТО / А.И. Ходанов. – DOI 10.33184/pravgos-2024.3.18 // Правовое государство: теория и практика. – 2024. – № 3. – С. 155–159.

Abstract. *The article analyzes the problems associated with recognizing a cyberattack on a NATO member state as a reason to declare war (casus belli). The article reveals the evolution of the Alliance's approaches to the issues of cyber threats and cyber defense from the Prague Summit in 2002 to the Brussels Summit in 2021. The article discusses the criteria proposed in the Tallinn Manual on the International Law Applicable to Cyber Warfare that make it possible to classify a cyberattack as an act of use of force. Statistics on cyberattacks are presented and their relevance to international law and cybersecurity is noted. Purpose: to analyze the conditions and circumstances under which a cyberattack may be considered by NATO countries as a reason to declare war. Methods: formal-legal, historical-systemic, retrospective. Results: the study has led to the following conclusions. First, despite existing international legal norms, the criteria for recognizing a cyberattack as a casus belli remain unclear, which allows NATO countries to retain flexibility in responding to cyber threats. Second, the application of Article 5 of the North Atlantic Treaty by NATO countries does not oblige them to unconditionally and without alternative to launch armed actions against the source state, but only requires other NATO members to provide any possible and appropriate assistance to the affected party.*

Keywords: *casus belli, cyberattack, cyber operation, international law, NATO, summits, Tallinn Manual*

For citation: Khodanov A.I. Challenges of Granting the Status of Casus Belli to a Cyberattack on a NATO Member State. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2024, no. 3, pp. 155–159. (In Russian). DOI 10.33184/pravgos-2024.3.18.

Введение

Актуальность проблемы придания статуса casus belli кибератаке на государство – члена НАТО предопределена взаимоувязанными причинами политического и технологического характера. Начиная с 2002 г. страны Североатлантического союза в рамках официальных встреч, переговоров и иных формальных и неформальных коммуникаций периодически рассматривают различные аспекты этой проблемы. В эти же годы существенно увеличилось разнообразие, результативность и массовость кибератак: доступность сложных информационно-коммуникационных технологий привела к существенному увеличению быстроты и эффективности действий атакующих, а стремительное распространение общедоступных средств электронных коммуникаций предоставило начинающим киберпреступникам актуальную информацию о сложных технологиях атак и свободный доступ к разнообразным программным инструментам их реализации. Новой угрозой нашего времени стала технология генеративного искусственного интеллекта, позволяющая киберпреступникам быстро находить уязвимости информационных систем и средств их защиты. Как результат, в условиях сложной внешнеполитической обстановки сегодня, как никогда ранее, существенно возрастает риск признания некоторой особо эффективной кибератаки на государство – члена НАТО не просто кибератакой, а casus belli (поводом к войне).

Кибератаки в цифрах

Статистика кибератак демонстрирует различающиеся численные показатели, что связано с особенностями оснований классификации кибератак, методов их учета и источников обрабатываемой информации. Вместе с тем любые статистические данные в среднем правильно отражают тренды киберпреступности, вследствие чего могут быть использованы для научного анализа. По данным исследователей проблем кибербезопасности[1], в 2023 г. по сравнению с 2022 г. количество пользователей, чьи учетные и персональные данные были похищены и попали на специализированные сайты, осуществляющие продажи таких данных, выросло на 76 %; количество предложений посредников о предоставлении на коммерческой основе несанкционированного доступа к сетевым ресурсам увеличилось на 20 %; среднее время активности атакующего в вычислительной системе после успешного проникновения в нее сократилось с 84 до 62 минут; количество результативных атак на облачные ресурсы с 2022 по 2023 г. выросло на 75 %; во второй половине 2023 г. количество кибератак выросло на 73 % по сравнению с 2022 г.; доля атак без использования вредоносного программного обеспечения составила 75 % в 2023 г. по сравнению с 71 % в 2022 г.

Эволюция взглядов НАТО на кибератаки

Подобная динамика кибератак была предсказуема, а ущерб от них признан значительным еще в начале 2000-х годов, вследствие чего в 2002 г. в п. 4 Декларации Пражского саммита появилось первое упоминание о кибератаках на страны Североатлантического союза как об общей угрозе, которую необходимо принимать во внимание[2]. Впоследствии, в 2014 г., в п. 72 Декларации Уэльского саммита впервые было закреплено следующее юридически значимое положение: «Наша политика также признает, что международное право, включая международное гуманитарное право и Устав ООН, применяется в киберпространстве. Кибератаки могут достигать порога, угрожающего национальному и евроатлантическому процветанию, безопасности и стабильности. Их воздействие может быть таким же вредным для современных обществ, как и обычная атака. Поэтому мы подтверждаем, что киберзащита является частью ключевой задачи НАТО по коллективной обороне. Решение о том, когда кибератака приведет к применению статьи 5, будет приниматься Североатлантическим советом в каждом конкретном случае»[3].

1 Глобальный отчет об угрозах CrowdStrike 2024 [Электронный ресурс]. URL: https://www.crowdstrike.com/global-threat-report (дата обращения: 30.06.2024).

2 Декларация Пражского саммита [Электронный ресурс]. URL: https://www.nato.int/cps/en/natohq/official_texts_19552.htm (дата обращения: 30.06.2024).

3 Декларация Уэльского саммита [Электронный ресурс]. URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm (дата обращения: 30.06.2024).

В 2016 г. в п. 70 Коммюнике Варшавского саммита страны Североатлантического союза декларировали новую парадигму – киберпространство, которое имеет такую же стратегическую важность, как воздушное пространство, суша и море: «Сейчас, в Варшаве, мы … признаем киберпространство областью операций, в которой НАТО должно защищать себя так же эффективно, как в воздухе, на суше и на море»[4]. При этом распространение порядка применения ст. 5 Североатлантического пакта на инциденты именно в киберпространстве не было декларировано. Однако уже в 2021 г. в п. 32 Коммюнике Брюссельского саммита было закреплено следующее положение: «Киберугрозы безопасности Североатлантического союза являются сложными, разрушительными, принудительными и становятся все более частыми. Недавно это было проиллюстрировано инцидентами с программами-вымогателями и другой вредоносной кибер активностью, нацеленной на нашу критически важную инфраструктуру и демократические институты, которые могут иметь системные последствия и нанести значительный ущерб. Чтобы противостоять этому развивающемуся вызову, мы сегодня одобрили всеобъемлющую политику НАТО в области киберзащиты, которая будет поддерживать три основные задачи НАТО и общую стратегию сдерживания и обороны, а также еще больше повысит нашу устойчивость. Подтверждая оборонительный мандат НАТО, Североатлантический союз полон решимости постоянно использовать весь спектр возможностей для активного сдерживания, защиты от всего спектра киберугроз и противодействия им, включая те, которые осуществляются в рамках гибридных кампаний в соответствии с международным правом. Мы подтверждаем, что решение о том, когда кибератака приведет к применению статьи 5, будет приниматься Североатлантическим советом в каждом конкретном случае»[5].

Таким образом, согласно рассмотренным документам, кибератака не становится автоматически casus belli, но лишь потенциальным «конкретным случаем», который будет рассматриваться Североатлантическим советом, определяющим уровень и содержание ответного реагирования. Такой подход не указывает на непроработанность странами НАТО проблемы реагирования на кибератаки. Напротив, Североатлантический союз умышленно оставил неуточненными и непоясненными критерии критичности кибератак и меры реагирования на них, тем самым развязывая себе руки для объявления инициатором атаки любого государства, оставляя возможность учета «политической» и иных составляющих оценки кибератаки, скрытой подготовки ответа, имеющего любую степень жесткости и любой масштаб. Подтверждение этому – публичное заявление Генерального секретаря НАТО Йенса Столтенберга, сделанное в 2018 г.: «Меня часто спрашивают, при каких обстоятельствах НАТО применила бы статью 5 в случае кибератаки. Мой ответ: посмотрим. Уровень кибератаки, который может спровоцировать ответ, должен оставаться целенаправленно неопределенным. Как и характер нашего ответа»[6].

Критерии кибератак как casus belli в Таллиннском руководстве

И все же, имеются ли иные источники определения критериев кибератак как casus belli? Ответ на этот вопрос положительный. В качестве основного такого источника выступает Таллиннское руководство по международному праву, применимому при ведении кибервойны, разработанное международной группой экспертов по заказу Центра передового опыта НАТО по совместной защите от киберугроз и опубликованное в первоначальной редакции в 2013 г.[7]

4 Коммюнике Варшавского саммита [Электронный ресурс]. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (дата обращения: 30.06.2024).

5 Коммюнике Брюссельского саммита [Электронный ресурс]. URL: https://www.nato.int/cps/en/natohq/news_185000.htm (дата обращения: 30.06.2024).

6 Столтенберг представил подробности киберполитики НАТО [Электронный ресурс] // Атлантический совет : сайт. URL: https://www.atlanticcouncil.org/blogs/natosource/stoltenberg-provides-details-of-nato-s-cyber-policy (дата обращения: 30.06.2024).

7 Таллиннское руководство по международному праву, применимому к кибервойне [Электронный ресурс]. URL: https://d-russia.ru/wp-content/uploads/2013/08/tallinnmanual.pdf (дата обращения: 30.06.2024).

Последовательность логических и юридических заключений в Таллиннском руководстве закреплена в Правилах, которые демонстрируют тезисы, посылки и выводы на их основе, позволяющие классифицировать инцидент компьютерной безопасности или как кибератаку, или как акт кибервойны.

Чтобы разграничить нормы информационной безопасности и нормы, относящиеся к кибервойне, Таллиннское руководство применительно к кибервойне в Правиле 11 вводит следующее определение кибероперации: «применение силы, когда ее масштаб и последствия сопоставимы с не-кибероперациями, достигающими уровня применения силы». В Правиле 13 добавлено, что «вопрос о том, является ли кибероперация вооруженным нападением, зависит от ее масштаба и последствий».

Поскольку отнесение кибероперации к акту кибервойны проводится с учетом критерия применения силы, Таллиннское руководство дает свое толкование составляющих кибероперации, позволяющих в совокупности относить конкретную кибероперацию к акту кибервойны. Первой из них названо государственное участие. На наш взгляд, именно эта составляющая наиболее неоднозначна. Подмена IP-адресов, преднамеренное формирование цифровых следов в файлах, ложно указывающих на носителя языка, страну и иные существенные обстоятельства создания файлов, возможность проведения в сети Интернет информационных операций с целью распространения дезинформации о государственном участии делают крайне спорными выводы специалистов о государственном участии в кибероперации в каждом конкретном случае.

Второй составляющей названа содержательная часть кибероперации. И эта составляющая заведомо противоречива, так как закрепленные в национальных законодательствах действия, квалифицируемые как киберпреступления, явно не могут быть трактованы расширительно как акт кибервойны. При этом, согласно международному праву, все иные не запрещенные явно действия считаются законными и тоже не могут быть трактованы как компоненты акта кибервойны.

Более понятна формулировка третьей составляющей, в качестве которой выступают особенности объекта атаки. Чем выше уровень защищенности атакованной информационной системы, тем более вероятно, что она является военным объектом или объектом критической инфраструктуры, вследствие чего деструктивные действия в отношении нее могут быть квалифицированы как акт кибервойны.

К четвертой составляющей Таллиннское руководство относит быстротечность проведения кибероперации. Считается, что конкретная кибероперация имеет тем большую вероятность быть признанной актом кибервойны, чем быстрее она достигает результата и чем меньше предоставляет возможности атакуемому ликвидировать нанесенный ущерб.

В целом Таллиннское руководство, как и иные источники норм современного международного права, не содержит однозначного ответа на вопрос о том, что именно считается casus belli в киберпространстве. В результате этой неопределенности инициатор конкретной кибероперации может считать свои действия обычной кибератакой, тогда как атакуемый может воспринимать происходящее как акт кибервойны. Как следствие, такие действия могут быть признаны атакуемой стороной как casus belli вопреки всем разъяснениям экспертов в области международного права. При этом считать такую оценку юридически обоснованной и использовать ее в качестве повода для войны на практике не получится даже у государства, ставшего целью кибероперации.

Заключение

Завершая рассмотрение проблемы придания статуса casus belli кибератаке на государство – члена НАТО, следует заметить, что ст. 5 Североатлантического договора вовсе не требует в безусловном и безальтернативном порядке начать вооруженные действия против государства, определенного странами НАТО в качестве государства – источника атаки. Эта статья скорее лишь обязывает дру-

гих членов НАТО оказать любую возможную и надлежащую помощь пострадавшей стороне. С важной оговоркой о том, что об этих мерах немедленно извещается Совет Безопасности ООН, принятие таких мер должно быть прекращено, как только Совет Безопасности ООН примет меры, необходимые для восстановления и сохранения международного мира и безопасности[8].

8 Североатлантический договор (Вашингтон, Федеральный округ Колумбия, 4 апреля 1949 г.) [Электронный ресурс]. URL: https://www.mid.ru/upload/archive/518ef5100baca933acb7a46d058d5c68.pdf (дата обращения: 30.06.2024).

Информация об авторе

Ходанов Андрей Иванович – кандидат юридических наук, директор Института правоохранительной деятельности.

Information about the Author

Khodanov Andrei Ivanovich – Candidate of Sciences (Law), Director of the Institute of Law Enforcement.

Статья поступила в редакцию 05.07.2024; одобрена после рецензирования 31.07.2024; принята к публикации 31.07.2024.
The article was submitted 05.07.2024; approved after reviewing 31.07.2024; accepted for publication 31.07.2024.