УДК 34

Киберхалифат: нормативное определение и криминологическая характеристика в национальном и международном информационном праве

Аббуд Руслан Ратебович

Главный специалист, юрист 3 класса,
Судебный департамент при Верховном Суде Российской Федерации,
107996, Российская Федерация, Москва, ул. Гиляровского, 31-2;
e-mail: Ruslan625@yandex.ru

Аннотация

В настоящей статье предпринята попытка раскрыть сущность Киберхалифата. Автор дает определение этой группе интернет-террористов, анализирует их цели, мотивы. Выясняет, какими правовыми средствами можно оказать воздействие на кибертерроризм в целом. На основе анализа автор пришел к выводу о необходимости выработки на международном уровне дефиницию кибертерроризма. По мнению автора, кибертерроризм можно отнести к преступлениям международного характера, когда предполагаемые злоумышленники и их жертвы находятся в разных государствах. Кибертерроризм это один из новых видов вызовов и угроз для всего мирового сообщества. Эта проблема носит весьма глобальный характер, и она будет неуклонно нарастать по мере развития и распространения информационных технологий. В связи с этим эффективное международное сотрудничество в области предупреждения и ликвидации последствий кибератак имеет огромное значение, так как контролировать кибертерроризм и бороться с ним на уровне отдельного государства представляется практически невозможным. Принятие международных норм и стандартов должно сопровождаться внесением изменений в национальное законодательство государств. Координация усилий государств необходима для обеспечения быстрого реагирования на развитие компьютерных технологий и принятия соответствующих норм.

Для цитирования в научных исследованиях

Аббуд Р.Р. Киберхалифат: нормативное определение и криминологическая характеристика в национальном и международном информационном праве // Вопросы российского и международного права. 2018. Том 8. № 8А. С. 190-197.

Ключевые слова

Киберхалифат, кибертерроризм, международная информационная безопасность, Министерство иностранных дел Российской Федерации; Соединенные Штаты Америки, Российская Федерация.

Введение

Киберпреступность является современным вызовом, который исходит от негосударственных акторов. По сравнению с другими вызовами, такими как международный терроризм, транснациональная организованная преступность, киберпреступность является новой угрозой. Официальная позиция Российской Федерации заключается в том, что существует проблема международной информационной безопасности. Этот термин еще не является повсеместно признанным. В ряде западных стран говорят больше о кибербезопасности. Под кибербезопасностью подразумевается прежде всего безопасность сетей.

Основная часть

По мнению директора департамента по вопросам новых вызовов и угроз МИД России Рогачева И.И. в Российской Федерации международная информационная безопасность включает в себя три элемента:

1) Это военно-политическая составляющая. Можно нанести ущерб государству за счет кибератак не меньше, чем бомбардировками;

2) Можно вывести из строя экономический объект, инфраструктуру, лишить государства управления;

3) Отдельный аспект — это кибертерроризм, который, в свою очередь, включает две составляющие. Во-первых, это террористические атаки на сети, что, собственно, и понимается как кибербезопасность. Другой аспект — это использование интернета для распространения террористической идеологии, пропаганды терроризма.

Рассмотрим третий аспект международной информационной безопасности более подробно.

Группировка интернет-террористов − Киберхалифат, которая является подразделением «Исламского государства» (запрещенная в Российской Федерации террористическая организация) взломала аккаунт центрального командования вооруженных сил США в социальной сети «Twitter» и популярном видеохостинге «Youtube». Кибертеррористы выложили в открытый доступ секретные сведения о военнослужащих армии США, включая их позывные и телефонные номера. Спустя некоторое время злоумышленники совершили террористическую атаку на запись издания «Newsweek» в «Twitter». На странице портала в сети микроблогов появилось несколько сообщений с угрозами, одно из которых было адресовано первой леди США, ее дочерям и мужу. «КиберХалифат объявляет киберджихад в виртуальном пространстве Интернет. В то время как США и их союзники убивают наших братьев в Сирии, Ираке и Афганистане, мы намерены уничтожить их системы кибербезопасности. Мы и дальше намерены продолжать атаку на сеть Пентагона» − говорится в оставленных кибертеррористами посланиях [Голубев, www].

Данное преступление можно квалифицировать по части 1 статьи 2 (Противозаконный доступ), Главы II Конвенции Совета Европы « О преступности в сфере компьютерной информации» (ETS № 185) (Будапешт, 23.11.2001) (далее – Конвенция от 23.11.2001), статья 3 (Распространение расистских и ксенофобских материалов посредством компьютерных систем), статья 4 (Мотивированная угроза расизма и ксенофобии), Главы II Дополнительного Протокола № 1 к Конвенции от 23.11.2001 [Доктрина, www]. Помимо взлома базы данных и незаконного доступа к персональной информации, террористы-хакеры Киберхалифата используют стремительно развивающиеся технологии, информационные инструменты для пропаганды

деструктивных идеологий, инструменты рекрутинга и насаждения насилия для усиления восприятия их действий. Они демонстративно показывают свои действия для того, чтобы посеять страх у своих оппонентов и обеспечить себе поддержку. Они используют специальные кибер-инструменты для распространения террора. Агитация и вербовка в свои ряды является подстрекательством к насильственным действиям и распространением экстремистской информации и подпадает под статью 7 (Пособничество и подстрекательство), Главы II Дополнительного протокола к Конвенции по киберпреступлениям в отношении криминализации деяний расистского и ксенефобского характера, осуществляемых при помощи компьютерных систем (г. Страсбург, 28.01.2003). Также путем обмена информацией через всемирную паутину и сети связи, координируются и осуществляются террористические акты. Одна из основных идей Конвенции от 23.11.2001 является определение единообразных составов компьютерных преступлений, которые государства должны включить в свои национальные законодательства, а также разработка мер борьбы с ними. Террористы «ДАИШ» (запрещенная в Российской Федерации террористическая организация) стараются вербовать в свои ряды молодых людей (средний возраст 23 года), а также военных специалистов, лингвистов и переводчиков. Через сайты это им сделать на территории нашей страны затруднительно, так как Роскомнадзор сразу блокирует их и вносит в черный список. Поэтому кибертеррористы используют социальные сети и чаты. В течение 2001-2005 года Российская Федерация активно участвовала в разработке проекта Конвенциии Совета Европы о предупреждении терроризма (CETS № 196) (Варшава, 15.05.2005) (далее − Конвенция от 16.05.2005) и первым ратифицировала его 21.04.2006. Согласно Конвенции от 16.05.2005 впервые в мировой практике подстрекательство к терактам (статья 5), а также вербовка (статья 6) и подготовка террористов (статья 7) признаны уголовными преступлениями.

В своей резолюции от 17.12.2015 Совет Безопасности ООН, выражая озабоченность по поводу того, что в глобализированном обществе террористы и их сторонники все шире используют новые информационно-коммуникационные технологии, в частности Интернет, для содействия террористическим актам, и осуждая использование этих технологий в целях подстрекательства, вербовки, финансирования или планирования террористических актов, выражая озабоченность по поводу международной вербовки новых членов в ряды «ИГИЛ» (запрещенная в Российской Федерации террористическая организация), «Аль-Каиды» и связанных с ними групп и масштабов этого явления и ссылаясь на свою резолюцию 2178 (2014), в которой Совет постановил, что государства-члены должны в соответствии с международными стандартами в области прав человека и нормами международного беженского права и международного гуманитарного права предотвращать и пресекать вербовку, организацию, перевозку и экипировку иностранных боевиков-террористов и финансирование деятельности [Иванов, 2013]. Предотвращение международной вербовки новых членов в ряды террористов является на сегодняшний день актуальным вопросом для всего мирового сообщества. Террористы настолько активно используют интернет для коммуникации, рекрутирования, пропаганды и сбора средств, что нанесение упреждающего удара является просто необходимой мерой для предотвращения кибертерроризма. Государства, поддерживающие упреждающие удары, имеют достаточные основания для использования кибер-оружия для того, чтобы сорвать планирование и подготовку террористического акта через сети ЭВМ. Вопрос о применения кибер-оружия как предупредительной меры стоит вынести на рассмотрение ООН. Тем самым узаконив данную меру на международном уровне борьба против кибертерроризма станет более эффективной.

Стремительные темпы освоения цифрового пространства и внедрение новых технологий привели к тому, что Конвенция от 23.11.2001 перестала быть актуальной. В период ее разработки (1997-2001 гг.) о многих угрозах в сфере информационной безопасности, включая некоторые уголовные преступления, не было известно, либо им не придавалось должного значения. На сегодняшний день появились новые виды преступлений в сфере информационных технологий, в частности использование злоумышленниками так называемых «ботнетов» – сетей компьютеров, зараженных вредоносной программой, которая позволяет удаленно выполнять различные противоправные действия. Также в качестве примера можно привести отсутствие ссылок в Будапештской Конвенции на принятие антиспамовских мер, «фишинг» и др. Сложно эффективно вести борьбу с новыми проявлениями терроризма в информационном пространстве без его юридического определения и, соответственно, криминализации как самого понятия, так и его составляющих [Тропина, 2005]. Таким образом, необходим документ глобального охвата по борьбе с преступностью в информационной сфере, который гарантировал бы суверенитет и невмешательство во внутренние дела государств посредством ЭВМ.

До сих пор как в национальном, так и в международном праве отсутствует легальное определение кибертерроризма. В отечественной юридической литературе ряд авторов дали киберртероризму дефиницию. Например, Голубев В.А. понимает под кибертерроризмом: «преднамеренную, политически мотивированную атаку на информацию обрабатываемою компьютером, компьютерную систему и сети, которая создает опасность для жизни или здоровья людей или наступления других тяжких последствий, если такие действия были содеянные с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта» [Голубев, www]. А что представляет из себя Киберхалифат, который выступает субъектом вышеупомянутого кибертерроризма? Организованная преступная группировка, совершающая преступления в сфере компьютерной информации? Внося собственный вклад в дефиницию рассматриваемого понятия, автор статьи считает возможным определить Киберхалифат − как террористов, взламывающих информационные системы для создания эффекта опасности, которую можно использовать для политического воздействия. Своими кибератаками они пытаются посеять страх, хаос и дестабилизировать обстановку в стране.

В Киберхалифат входят в основном граждане Бельгии, Франции, Великобритании и иных европейских государств, которые имеют специальные зачатки знаний в области компьютерной информации и в связи с этим они очень быстро осваивают новые достижения в области информационных технологий у стран Западной Европы и США и в дальнейшем используют инновации против них. «ДАИШ» (запрещенная в Российской Федерации террористическая организация) впервые взяла на себя ответственность за терракты в Париже через использование популярной услуги, мгновенного обмена сообщениями, приложения «Telegram». Это приложение позволяет шифровать сообщения с обеих сторон. В результате спецслужбам затруднительно вычислить злоумышленников и заблокировать обмен информации.

Для успешного противодействия киберпреступности, в частности, кибертерроризму, необходимо принять следующие меры:

1) Установить эффективное международное сотрудничество с иностранными государствами, их спецслужбами и правоохранительными органами, а также организовать тесный контакт с международными организациями для скорейшего разрешения данной проблемы.

2) Принять необходимые законы о защите компьютерной безопасности в соответствии с действующими международными стандартами и конвенциями Совета Европы.

3) Создать специальные подразделения (Киберполиция) как на национальном, так и на международном уровне для эффективной борьбы с киберпреступностью.

Говоря о мерах борьбы против кибертерроризма, стоит также затронуть вопрос ответственности киберпреступников. Под юрисдикцию какого государства подпадают их преступления? Будут ли киберзлоумышленники привлечены к ответственности в соответствии с законодательством государства, из которого было совершено данное деяние или же по законодательству государства на которое это преступление было направлено? Возможна ли экстрадиция в данном случае? Вопрос весьма глобальный и требует решительных действий со стороны международных организаций. Международному сообществу следовало бы выработать юридически-обязательное консолидированное решение по данному вопросу.

Такие сверхдержавы, как Российская Федерация и США принимают активное участие в противодействие киберпреступности в целом. Указом Президента РФ от 15 января 2013 г. №31 с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» на ФСБ Российской Федерации возлагаются полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы Российской Федерации, информационные системы и информационно-телекоммуникационные сети, находящиеся на территории РФ и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом. В связи с возникновением новых военных опасностей и угроз была обновлена Доктрина информационной безопасности Российской Федерации 2000 года. Новая Доктрина была утверждена Указом Президента РФ от 5 декабря 2016 г №646. Основными направлениями обеспечения информационной безопасности в области обороны страны называются «стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий», и «совершенствование системы обеспечения информационной безопасности» Вооруженных сил. В свою очередь, президент США в октябре 2012 года подписал Директиву № 20 (Presidental Policy Directive 20) обязывающую создать систему кибербезопасности страны и разработать стандарты и методики, которые помогут снизить риски от кибератак на самые важные объекты инфраструктуры.

В настоящее время происходит формирование системы международной информационной безопасности. Международная информационная безопасность межгосударственной системы является составной частью всеобъемлющей системы международной безопасности. Вместе с тем международная информационная безопасность является одним из стабилизирующих факторов системы международных отношений невластного характера. При этом ряд угроз международной информационной безопасности затрагивает сферу как международных властных, так и не властных отношений.

Заключение

Подводя итоги вышесказанному, следует отметить, что «ДАИШ» (запрещенная в Российской Федерации террористическая организация) и в дальнейшем будет учитывать использование информационных технологий и пытаться расширить свои технические

возможности в киберпространстве. Ведь взлом базы данных это только начало. В дальнейшем террористы-хакеры планируют атаки на финансовую систему и инфраструктуру США стран Запада. Ведь сегодня на черном рынке можно приобрести продвинутые технологии взлома компьютеров и целых сетей, поэтому из рук криминала такие технологии вполне могут попасть в руки к террористам. На данный момент мы наблюдаем как набирает обороты информационная война, где в отличие от традиционной войны, где воюют боевым оружием, в виртуальной многое зависит от электронных устройств и информации. Кибертерроризм один из новых видов вызовов и угроз для всего мирового сообщества. Эта проблема носит весьма глобальный характер и она будет неуклонно нарастать по мере развития и распространения информационных технологий. В связи с этим эффективное международное сотрудничество в области предупреждения и ликвидации последствий кибератак имеет огромное значение, так как контролировать кибертерроризм и бороться с ним на уровне отдельного государства представляется практически невозможным. Принятие международных норм и стандартов должно сопровождаться внесением изменений в национальное законодательство государств. Координация усилий государств необходима для обеспечения быстрого реагирования на развитие компьютерных технологий и принятия соответствующих норм.

Библиография

1. Голубев В.А. Кибертерроризм-угроза национальной безопасности. URL: http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism
2. Доктрина информационной безопасности Российской Федерации № 646 от 5 декабря 2016 года. URL: http://docs.cntd.ru/document/420384668
3. Дополнительный протокол к Конвенции по киберпреступлениям в отношении криминализации деяний расистского и ксенофобского характера , осуществляемых при помощи компьютерных систем (г. Страсбург, 28 января 2003 г.).
4. Иванов С.М. Международно-правовое регулирование борьбы с кибертерроризмом // Право и безопасность. 2013. № 3-4. С. 82-87.
5. КиберХалифат угрожает семье Обамы в Twitter (перевод автора с арабского языка). URL: http://www.alhakea.com/word/?p=30455
6. Конвенция Совета Европы «О преступности в сфере компьютерной информации» (ETS №185), (Будапешт, 23 ноября 2001 года).
7. Конвенция Совета Европы «О предупреждении терроризма» (CETS №196),(Варшава, 16 мая 2005 г.).
8. Крутских А., Стрельцов А. Международное право и проблема обеспечения международной информационной безопасности. URL: https://interaffairs.ru/jauthor/material/1167
9. Резолюция Совета Безопасности ООН 2253 от 17 декабря 2015 г. «Угрозы международному миру и безопасности, создаваемые террористическими актами».
10. Талимончик В.П. Международно-правовое регулирование отношений в сфере информации: автореф. дис. … докт. юр. наук. СПб., 2013. 39 с.
11. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры: автореф. дис. … канд. юр. наук. Владивосток, 2005. 19 с.
12. Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».
13. Хусам аль-Таи. Информационная война (пер. автора с арабского). URL: http://elaph.com/Web/opinion/2015/3/987803.html
14. Что мы знаем о кибернетических возможностях «ИГИЛ»? (перевод автора с арабского языка). URL: http://www.sasapost.com/translation/examining-the-islamic-states-cyber-capabilities
15. International Law Association. Study Group on Cybersecurity, Terrorism, and International Law. Overview of International Legal Issues and Cyber Terrorism. URL: www.ila-hq.org
16. Presidental Policy Directive № 20, signed by President Barack Obama in October 2012.
17. The National Military Strategy of the United States of America, 2015.

Cyber-Caliphate: normative definition and criminological characteristics in national and international information law

Ruslan R. Abbud

Senior Specialist, 3rd class lawyer,
Judicial Department of the Supreme Court of the Russian Federation,
107996, 31-2, Gilyarovskogo st., Moscow, Russian Federation;
e-mail: Ruslan625@yandex.ru

Abstract

In this article, an attempt is made to reveal the essence of Cyber-Caliphate. The author defines this group of Internet terrorists, analyzes their goals, motives. He finds out what legal means can affect the cyberterrorism in general. Based on the analysis, the author came to the conclusion that it is necessary to develop a definition of cyberterrorism at the international level. According to the author, cyberterrorism can be attributed to crimes of an international character, when alleged intruders and their victims are in different states. Cyberterrorism is one of the new types of challenges and threats for the entire world community. This problem is very global, and it will grow steadily as the development and dissemination of information technology. In this regard, effective international cooperation in the field of preventing and eliminating the consequences of cyber-attacks is of great importance, since it is practically impossible to control cyberterrorism and fight it at the level of an individual state. Adoption of international norms and standards should be accompanied by changes in the national legislation of states. The coordination of efforts of states is necessary to ensure a rapid response to the development of computer technology and the adoption of relevant standards.

For citation

Abbud R.R. (2018) Kiberkhalifat: normativnoe opredelenie i kriminologicheskaya kharakteristika v natsional'nom i mezhdunarodnom informatsionnom prave [Cyber-Caliphate: normative definition and criminological characteristics in national and international information law]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 8 (8A), pp. 190-197.

Keywords

Cyber-Caliphate, cyber-terrorism, cyber-attacks, the Ministry of Foreign Affairs of the Russian Federation, the USA, the Russian Federation.

References

1. Additional Protocol to the Convention on Cybercrime with regard to the criminalization of acts of a racist and xenophobic nature carried out by computer systems (Strasbourg, 28 January 2003).
2. Council of Europe Convention on Cybercrime in the Field of Computer Information (ETS No. 185), (Budapest, November 23, 2001).
3. Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), (Warsaw, 16 May 2005).
4. Cyber Caliphate threatens Obama's family on Twitter (author's translation from Arabic). Available at: http://www.alhakea.com/word/?p=30455 [Accessed 07/07/2018]

5. Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii № 646 ot 5 dekabrya 2016 goda [The Doctrine of Information Security of the Russian Federation No. 646 of December 5, 2016]. Available at: http://docs.cntd.ru/document/420384668 [Accessed 07/07/2018]
6. Golubev V.A. Kiberterrorizm-ugroza natsional'noi bezopasnosti [Cyberterrorism is a threat to national security]. Available at: http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism [Accessed 07/07/2018]
7. Husam al-Tay. Information war (author's translation from Arabic). Available at: http://elaph.com/Web/opinion/2015/3/987803.html [Accessed 07/07/2018]
8. International Law Association. Study Group on Cybersecurity, Terrorism, and International Law. Overview of International Legal Issues and Cyber Terrorism. Available at: www.ila-hq.org [Accessed 07/07/2018]
9. Ivanov S.M. (2013) Mezhdunarodno-pravovoe regulirovanie bor'by s kiberterrorizmom [International legal regulation of the fight against cyberterrorism]. Pravo i bezopasnost' [Law and security], 3-4, pp. 82-87.
10. Krutskikh A., Strel'tsov A. Mezhdunarodnoe pravo i problema obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti [International law and the problem of ensuring international information security]. Available at: https://interaffairs.ru/jauthor/material/1167
11. Presidental Policy Directive № 20, signed by President Barack Obama in October 2012.
12. Talimonchik V.P. (2013) Mezhdunarodno-pravovoe regulirovanie otnoshenii v sfere informatsii. Doct. Dis. [International legal regulation of relations in the field of information]. St. Petersburg.
13. (2015) The National Military Strategy of the United States of America.
14. Tropina T.L. (2005) Kiberprestupnost': ponyatie, sostoyanie, ugolovno-pravovye mery. Doct. Dis. [Cybercrime: concept, state, criminal law measures. Doct. Dis.]. Vladivostok.
15. Ukaz Prezidenta RF ot 15 yanvarya 2013 g. № 31s «O sozdanii gosudarstvennoi sistemy obnaruzheniya, preduprezhdeniya i likvidatsii posledstvii komp'yuternykh atak na informatsionnye resursy Rossiiskoi Federatsii» [Presidential Decree of January 15, 2013 No. 31c “On the establishment of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation”].
16. UN Security Council Resolution 2253 of December 17, 2015 “Threats to international peace and security caused by terrorist acts”.
17. What do we know about the cybernetic possibilities of ISIS? (translation of the author from Arabic). Available at: http://www.sasapost.com/translation/examining-the-islamic-states-cyber-capabilities [Accessed 07/07/2018]