МЕЖДУНАРОДНОЕ ПРАВО И СРАВНИТЕЛЬНОЕ ПРАВОВЕДЕНИЕ

УДК 343.34
ББК 67.408.135

КИБЕРТЕРРОРИЗМ КАК ОРУЖИЕ В ГИБРИДНОЙ ВОЙНЕ

В. А. Мазуров, М. А. Стародубцева
Алтайский государственный университет (Барнаул, Россия)

Рассматривается новая разновидность терроризма, действующего в виртуальном пространстве. Выдвигается тезис о том, что сегодня преступность в сфере высоких технологий может расцениваться как новый вид оружия. Авторы анализируют возможности и направления воздействия кибертерроризма на важнейшие объекты инфраструктуры и психофизиологическое состояние граждан. Делается вывод о том, что кибертерроризм в современных условиях фактически становится глобальным оружием так называемой гибридной войны в информационном пространстве.

Ключевые слова: кибертерроризм, информационное оружие, вербовка, хакерские атаки, политическое противодействие.

CYBER TERRORISM AS A WEAPON IN A HYBRID WAR

V. A. Mazurov, M. A. Starodubtseva
Altai State University (Barnaul, Russia)

The article discusses a new kind of terrorism operating in the virtual space. The thesis is advanced that today high-tech crime can be considered as a new type of weapon. The authors analyze the possibilities and directions of the impact of cyber terrorism on the most important infrastructure objects and the psychophysiological state of citizens. It is concluded that under modern conditions cyber terrorism is actually becoming the global weapon of the so-called hybrid war in the information space.

Keywords: cyber terrorism, information weapon, recruitment, hacker attacks, political opposition.

Doi: https://doi.org/10.14258/ralj(2020)1.11

Проблема определения термина «кибертерроризм»

Прежде чем подвергнуть анализу рассматриваемую нами тему постиндустриального общества, необходимо разобраться с применяемой терминологией. Как определяется кибертерроризм?

В 1997 г. сотрудник ФБР Марк Поллитт предложил считать кибертерроризмом любую умышленную политически мотивированную атаку на информацию, компьютерные системы, программы и данные, которые приводят к насилию в отношении невоенных целей, групп населения или тайных агентов [1, с. 19].

Необходимо подчеркнуть, что в юридической науке нет однозначного определения кибертерроризма. В массиве российской уголовной практики указанный вид преступности в чистом виде не встречается, чаще он связан с классическими формами терроризма: химическим, биологическим, транспортным и другими.

На данный момент можно выделить две основные точки зрения на кибертерроризм. Сторонники первого подхода под терроризмом в виртуальной среде понимают совокупность противоправных действий, связанных с покушением на жизнь людей или рядом других действий, способствующих нарастанию напряженности в обществе с целью получения преимущества при решении политических, экономических или социальных задач. Иными словами, эта точка зрения рассматривает кибертерроризм достаточно широко, фактически смешивая его с обычными террористическими атаками.

Приверженцы второй точки зрения описывают его как преднамеренную атаку на информацию, обрабатываемую компьютерной системой, создающую опасность для жизни и здоровья людей, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта [2, с. 5]. Соответственно, этот подход можно считать более узким, конкретизирующим кибернетическую угрозу. Однако здесь появляется опасность смешения терминов и отождествления кибертерроризма с информационным оружием.

Проанализировав основные аспекты дискуссии, мы предлагаем собственное определение терроризма в виртуальной среде. По нашему мнению, кибертерроризм есть многоаспектное явление, выражающееся в политически мотивированной атаке на виртуальную реальность, создающее опасность для жизни или здоровья людей либо наступления других тяжких последствий, связанное с нарушением общественной безопасности, запугиванием населения, подрывом инфраструктуры и провокациями военного характера.

Специфической чертой кибертерроризма является реальное, непосредственное воздействие на общество с целью его устрашения, распространения паники, чувства социальной незащищенности.

Конечной целью кибернетической атаки является, по нашему мнению, попытка оказать влияние на политическую власть в стране [3, с. 34].

По характеру воздействия на социум кибертерроризм практически универсален, так как возможен фактически в каждой сфере общества. Исходя из этого, авторы исследования выдвигают гипотезу о том, что сегодня киберпреступность и кибертерроризм можно рассматривать в качестве специфического вида оружия в противостоянии на международной арене и в борьбе с запрещенными террористическими организациями.

Современные направления кибертерроризма

Повторимся, что угроза, исходящая от кибертерроризма, огромна и может иметь необратимый характер. Современное общество еще стоит на пороге выработки эффективной системы противодействия и борьбы с киберпреступностью в террористической сфере, а следовательно, требуется тщательный анализ данного явления. Для начала выделим наиболее явные моменты, куда может нанести удар кибертеррорист.

Во-первых, работа современных инфраструктуры и коммуникаций невозможна без сети Интернет. Это следствие цифровизации общества и перехода на постиндустриальный уровень развития. Но это и причина повышенной уязвимости систем, объединенных одной компьютерной сетью [4, с. 41].

Сегодня наиболее уязвимыми точками инфраструктуры могут быть телекоммуникации, энергетика, авиационные диспетчерские, финансовые электронные и правительственные информационные системы, а также автоматизированные системы управления войсками и оружием [5, с. 12]. Обычно атаки кибертеррористов направлены на основные объекты национальной информационной инфраструктуры, такие как оборудование, включая персональные компьютеры пользователей и программное обеспечение объектов инфраструктуры.

Наиболее опасными по масштабу возможных разрушений нам видятся атаки на систему информационной защиты атомных электростанций. Первой зарегистрированной кибернетической атакой на подобный объект можно считать инцидент 1994 г. на Игналинской АЭС. Вычислительная система «Титан», обслуживающая эту станцию, подала роботам, работавшим на системе подачи ядерного топлива в один из реакторов, неверную команду. Практически следом пришло сообщение от не-

установленных лиц, что атомная станция будет взорвана, если некий обвиняемый будет приговорен к смертной казни. Благодаря оперативному и своевременному реагированию работа была остановлена [5, с. 28].

Необходимо отметить, что проблема ядерного терроризма в странах Запада была осознана еще в 1970-х гг. [5, с. 13]. Тогда еще она обсуждалась едва ли не на уровне фантастики и далекого будущего. В России данные вопросы не поднимались на законодательном уровне вплоть до настоящего времени, пока не началась практически повсеместная волна кибернетических атак.

Очередную кибератаку на объекты атомной энергетики зарегистрировали в 2010 г. в Иране, когда компьютерный червь STUXNET поразил работу ядерных центрифуг. Уникальность и опасность хакерской разработки заключалась в том, что впервые вирус смог разрушить инфраструктуру объекта на физическом уровне. По одной из версий, STUXNET — это продукт, созданный специалистами спецслужб США и Израиля с целью уничтожить надежды, связанные с ядерной программой Ирана [6, с. 29].

Приведенный пример ясно показывает, с одной стороны, беззащитность существующих ядерных энергетических объектов, а с другой — косвенно подтверждает факт использования кибертерроризма не только радикальными преступными группировками, но государствами. Кибертеррор в современных условиях является одним из способов борьбы на международной арене.

Возможности кибертерроризма как глобального оружия были продемонстрированы мировому сообществу 11 сентября 2001 г. Уже после серии терактов в своем интервью генерал-лейтенант ВВС США Эл Эдмондс сообщил, что перед атакой систему ПВО США на короткое время вывели из строя специалисты международного террориста Усамы Бен Ладена. После падения башен Всемирного торгового центра советник Белого дома по безопасности в киберпространстве назвал новую угрозу «цифровым Перл-Харбором».

Во-вторых, говоря об угрозах кибертеррористической преступности, следует понимать, что сегодня потенциальные мощности цифровой реальности активно используются не только запрещенными международными террористическими организациями, но и специалистами легитимных правительств. Например, давно работает и зарекомендовала себя возможность дистанционного перехвата систем управления военными спутниками, наведения и запуска ракет или комплексами противовоздушной обороны. Примером может служить вывод из строя систем ПВО Ирака во время операции «Буря в пустыне».

Используя замаскированные под террористические акты информационные атаки на иностранные государства, можно достигать тех целей, которые просто недостижимы законными методами политики и дипломатии. Это может быть подрыв экономики противостоящего государства, искусственное разжигание политической нестабильности, натравливание внутренней оппозиции в государстве друг на друга и на правящую власть или срывы важных международных договоренностей путем вброса дезинформации.

Здесь мы уже говорим о комплексном воздействии на противника различными средствами одновременно, которое в современной науке принято называть гибридной войной [7, с. 9].

Новизна нынешней информации и психологической войны — это двойная комбинация онлайн-СМИ. Этот тип «войны» постоянно продолжается, и его трудно обнаружить. Сложно определить его источник, поскольку чаще всего он осуществляется из нескольких источников одновременно. И, наконец, такая стратегия ведения войны проникает во все слои общества по очень низкой цене. Даже если аудитория не обязательно верит в заложенную информацию, обилие неподтвержденной информации само по себе ведет к постоянному недоверию к общественной информации и СМИ.

Томас Элькер Ниссен выделяет несколько военных мероприятий, в которых используются социальные сети: сбор разведывательных данных, таргетинг (умная реклама), психологическая война, наступательные и оборонительные кибероперации и деятельность по управлению и контролю.

Так, «Интеллектуальные агентства научились использовать социальные медиа в своих интересах. Используя поддельные идентификаторы, они могут создать иллюзию поддержки идей. Они также могут оспаривать идеи на платформах социальных сетей, вставляя встречные аргументы, которые, как представляется, исходят из “низового” уровня движения» [7, с. 41].

Элементом кибертерроризма, на наш взгляд, может выступать сегодня и так называемый сетевой троллинг. В данной работе мы попытались вывести собственное определение троллинга. Нами

он понимается как «размещение на различных ресурсах (форумах, социальных сетях и т. п.) провокационных сообщений с целью раздразнить участников дискуссии, вызвать конфликты между ними, спровоцировать взаимные оскорбления и т. д.». В свою очередь, гибридный троллинг — это метод ведения информационной войны посредством размещения провокационных сообщений в сети Интернет с целью внедрения пропагандистской идеологии.

Исследование интернет-троллинга было проведено активистами движений «Антиэкстремизм» и «Сообщество борьбы с национализмом» при поддержке Центра психологической безопасности в Санкт-Петербурге в 2018 г. При сборе информации использовались материалы методических рекомендаций НАТО по гибридному троллингу, находящиеся в свободном доступе в сети Интернет [7, с. 37].

В-третьих, не менее опасно и психологическое воздействие терроризма в цифровой среде на нравственное и психологическое состояние пользователей Интернета. Практически все современные террористические организации имеют тысячи сайтов и аккаунтов в социальных сетях, на которых размещаются материалы, носящие выраженный экстремистский характер.

Впервые Интернет с этой целью использовали боевики перуанской организации «Тупак Амару», когда в 1996 г. на приеме в японском посольстве они взяли в заложники несколько десятков человек. На созданных их единомышленниками пропагандистских сайтах журналистам предлагалось фактически в онлайн-режиме взять у лидеров группировки интервью о происходящих событиях. Бешеная активность прессы фактически реализовала задачи террористов. Необходимая боевикам информация была моментально распространена и растиражирована. Собственные интернет-публикации с угрозами и предупреждениями о готовящихся терактах первой стала осуществлять организация «Аль-Каида».

На данный момент практически все террористические организации используют мощный арсенал информационно-коммуникативных технологий [7, с. 48]. Наиболее известны из них видеоролики, широко растиражированные в Интернете, демонстрирующие показательные казни ИГИЛовцами заложников. Эти фильмы фактически произвели революцию в арабском сегменте Всемирной сети. Качество такого пропагандистского кинопродукта практически не уступает Голливуду.

Следует понимать, что показательные казни на камеру работают сразу в нескольких направлениях. И прежде всего это мощная самореклама, привлекающая внимание всего мира. Главная задача таких фильмов не только просто напугать зрителя, вселить ему чувство тревоги и страха, но и создать напряженную атмосферу постоянно нарастающего страха или мучительного ожидания чего-либо ужасного, вплоть до доведения до самоубийства.

Такое отношение к ИКТ со стороны радикалов объясняется радом причин. Во-первых, это относительно недорогое и одновременно весьма эффективное средство совершения акта терроризма, а во-вторых, в Интернете крайне сложно вычислить самого террориста. Наиболее активно методы информационного воздействия использует террористическое движение «Хезболла». Так, например, в структуре данной организации выделена группа программистов, в задачи которой входит создание и обновление веб-страницы в Интернете для пропаганды проводимых организацией акций и доведения направленной информации до израильтян [7, с. 19]. Возможность оказать серьезное морально-психологическое воздействие на общество побуждает террористов все чаще прибегать к Интернету, нежели традиционным методам борьбы с применением летального оружия.

Не менее действенным оказывается психологическое влияние на людей через массовые атаки вирусных программ на персональные компьютеры пользователей. Весной 2017 г. произошла массовая атака червей-вымогателей WannaCry. 75 000 компьютеров по всему миру, использующих систему Windows, были заражены вирусной программой. Она преимущественно нацеливалась на вымогательство, но и пыталась воспроизвестись на как можно большем количестве компьютеров в Сети.

На экраны мониторов выводилось объявление о вирусном нападении с требованием выкупа путем перевода денег на три кошелька криптовалюты биткоин. Чуть ниже отображался обратный отсчет времени, которое «осталось» у жертвы для выплаты выкупа и спасения информации.

Можно сказать, что своей непосредственной цели, а именно вымогательства, атака не достигла. Только один из тысячи зараженных компьютеров выплачивал выкуп хакерам. Но само нападение широко освещалось в мировых СМИ и социальных сетях, привлекло внимание спецслужб многих стран и стало ярким примером современного кибертерроризма [8, с. 5].

А ведь подобные атаки можно осуществить не только на персональные компьютеры. По подсчетам независимых экспертов Центра психологической безопасности (г. Санкт-Петербург), удар по сети Интернет и отключение компьютерных систем может привести к разорению 20% средних банковских компаний в течение нескольких часов, 48% компаний потерпят крах в течение нескольких суток. Еще около 33% банков будут разорены спустя несколько часов после такой катастрофы, а 50% из них разорятся спустя несколько суток [9, с. 16]. Несложно догадаться, что в условиях современной глобализации после такой атаки начнется новый мировой финансовый кризис.

Можно сделать промежуточный вывод о том, что по своим задачам терроризм в виртуальной среде ничем не отличается от классического террора, так как его главная цель в том, чтобы посеять страх и хаос среди населения.

В-четвертых, весьма опасным направлением кибертерроризма является оказание психофизиологического воздействия на отдельные социальные группы. Ярким примером, однако довольно сомнительным по качеству имеющейся о нем информации, служит так называемый вирус № 666, по мнению медиков, способный путем целенаправленного разрушения нервных центров организма привести к смерти оператора персонального компьютера. Принцип его действия основан на феномене так называемого 25-го кадра. Например, если в течение фильма к двадцати четырем кадрам в секунду добавить еще один — 25-й, несущий совсем другую информацию, то глаз человека его не заметит, однако сами данные неизбежно проникнут в мозг человека и будут им обработаны.

Судя по всему, по расчету авторов вируса, направленность восприятия изображения на подсознание и несовпадение полученных данных с информацией, поступающей непосредственно от органов чувств, должно вызывать резкие перепады сердечной деятельности, приводящие к перегрузке сосудов, вплоть до смерти от остановки сердца. По некоторым, однако не подтвержденным, данным, за последние несколько лет только в странах СНГ зафиксировано 46 случаев гибели операторов, работающих в компьютерных сетях, от подобного вируса [9, с. 37].

По мнению авторов, волна подростковых самоубийств, прокатившаяся по России и СНГ с 2015 по 2017 г., была также связана с использованием подобных технологий. Большинству участников социальных игр «Синий кит» и «Тихий дом» предлагалось не только поэтапно выполнять 50 аутоагрессивных заданий и выкладывать фотоотчет в Сеть, но и просматривать некие видеоролики, демонстрирующие, например, крушение поезда с многочисленными жертвами, взрывы жилых многоквартирных домов, пожары и массовые убийства. Такие ролики кураторы суицидальных групп требовали смотреть только в определенное время, чаще всего в 4:20 утра, когда мозг предельно расслаблен и заторможен. Можно увидеть именно в этом факте пресловутую технологию 25-го кадра. В результате подобного массированного воздействия подростки, не входящие в группу психологического риска, безропотно прыгали с крыш высотных зданий.

Случаи массовых суицидов, подобных «Синему киту», видятся нам вариантом гибридной войны. В данном случае это репетиция одного из этапов акций политического протеста. Так отрабатываются на практике технологии перекодирования сознания, оттачиваются приемы отключения критического мышления.

В-пятых, не менее важным направлением действий кибертеррористов является информационный вброс с целью нарушения баланса сил на международной арене и разжигания межнациональных конфликтов. Первые проявления подобного рода террора дезинформацией проявили себя еще в прошлом веке.

Сегодня наметилась тенденция связи многих кибертерактов с конкретными политическими заказами. Например, 9 мая 2014 г. мировая группа хакеров-активистов Anonymous на несколько часов фактически блокировала официальный портал Президента Российской Федерации Kremlin.Ru. Позже работа сайта восстановилась.

Специалисты по кибербезопасности указывают на то, что популярная технология видеоконференций, широко применяемая сегодня в государственном управлении и образовательной среде, весьма уязвима, поскольку с применением современных программ возможна полная фальсификация транслируемого изображения. Например, инженеры Массачусетского технологического института, прибегнув к помощи так называемой «нейросети», показали публике видеозаписи известных публичных деятелей. Их голоса были искусно сгенерированы машиной, но сами выступления кардинально отличались от реальных политических программ данных лиц [9, с. 31]. Такая технология

вполне способна привести к массовой дезинформированности населения и резкому падению политической стабильности в обществе внутри государства.

Все это доказывает высказанный нами тезис о возможности применения преступности в кибертеррористической сфере в качестве оружия гибридной войны.

Можно сказать, что сегодня киберотеррористы активно вмешиваются в международные политические отношения, совершая одиночные вбросы либо проводя долговременную агрессию против конкретных стран.

Так, например, в 2018 г. хакерская группа GhostShell объявила о начале кибервойны с Россией и опубликовала данные около 2,5 млн аккаунтов и различных записей взломанных учреждений по многим сферам общества. Операция именуется Project BlackStar и, по словам хакеров, направлена именно против российского правительства. Несколько ранее аналогичную кибервойну GhostShell развернула против Китая [9, с. 29].

Страны, претендующие на собственную исключительную роль в однополярном мире, судя по всему, вынуждены обращаться к методам информационного воздействия. В начале октября 2014 г. в США была обнародована новая оперативная концепция сухопутных американских войск «Победа в сложном мире. 2020–2040». При этом в концепции выделяют пять полей противоборства: суша, море, воздух, космос и киберпространство.

В-шестых, еще одно направление, где активно проявляет себя кибертерроризм, — это агитация, пропаганда и вербовка в свои ряды новых членов. По некоторым данным, только в Twitter зарегистрировано более 45 тыс. аккаунтов «Исламского государства» (запрещенного в России), что превращает их в мощный ресурс пропагандистской машины террористов. До недавнего времени именно здесь велось информирование пользователей об успехах ИГИЛ, проводился массовый сбор средств в поддержку военных действий группировки в Ираке и Сирии. В связи с этим мы можем вернуться к вопросу «групп смерти» и отметить, что вполне могла осуществляться вербовка в экстремистские и террористические организации кураторов данных сетевых объединений.

Современные технологии и методы набора сторонников в радикальные группировки значительно увеличили масштаб и результативность данного вида деятельности. Сегодня рекрутирование может осуществляться удаленно, посредством сети Интернет, когда традиционный контакт становится невостребован. С другой стороны, агитатор имеет возможность оказывать влияние одновременно на большое количество людей, проживающих по всему миру.

Классическим примером уже стала история студентки В. Карауловой, завербованной членами ИГИЛ и дважды попытавшейся проникнуть на территорию «Исламского государства».

Сложен вопрос и квалификации указанных выше преступлений. Большинство текстов террористов в Сети крайне сложно квалифицировать с точки зрения уголовного законодательства. В течение 2018 г. созданная авторами исследования волонтерская организация «Антиэкстремизм» сотрудничала с Центром противодействия экстремизму и пыталась мониторить потенциально экстремистские публикации в социальных сетях. Из шестнадцати обнаруженных и обработанных нами текстов лингвистическая экспертиза признала частично экстремистским всего один. Административное законодательство также не предусматривает ответственности именно за кибертерроризм.

Исходя из этого, предлагаем внести понятие «кибертероризм» в диспозицию ч. 2 ст. 280 УК РФ и в диспозицию ч. 3 ст. 205 УК РФ, тем самым обозначив новый вид преступлений в уголовно-правовом массиве.

Библиографический список

1. Агапов П. Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма: анализ законодательной новации // Уголовное право. 2007. № 1.

2. Экстремизм и его причины / под ред. Ю. М. Антоняна. М., 2010.

3. Обеспечение психологической безопасности в образовательном учреждении : практическое руководство / под ред. И. А. Баевой. СПб., 2006.

4. Борисов С. В., Жеребченко А. В. Квалификация преступлений экстремистской направленности : учеб. пособие / отв. ред. и предисл. засл. деят. науки РФ, д-ра юрид. наук, проф. Н. И. Ветрова. М., 2011.

5. Захаров А. В. Массовое общество и культура в России: социально-типологический анализ // Вопросы философии. 2003. № 9.

6. Погодин И. В. Преступления экстремистской направленности: методика доказывания / под науч. ред. и с предисл. д-ра юрид. наук., проф. Н. А. Колоколова. М., 2012.

7. Казанцев А. А. Проблемы вербовки и возврата боевиков-террористов: опыт Европы и перспективы России. М., 2016. № 27.

8. Выступление заместителя руководителя аппарата Национального антитеррористического комитета А. И. Ковалева // Вестник Национального антитеррористического комитета. 2017. № 1 (16).

9. Кубякин Е. О. К вопросу определения сущности экстремистских установок молодежи // Власть. 2010. № 9.