Научная статья
УДК 343.3/.7:004
EDN: https://elibrary.ru/hfpmtn
DOI: https://doi.org/10.21202/jdtl.2023.10

Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию

Елена Юрьевна Антонова

Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации
г. Владивосток, Российская Федерация

Ключевые слова

Вербовка,
криминализация,
право,
преступление,
пропаганда,
пространство,
противодействие,
терроризм,
финансирование,
цифровые технологии

Аннотация

Цель: выработка рекомендаций по противодействию преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

Методы: методологическую основу исследования составляют всеобщий диалектический метод познания, совокупность общенаучных и частнонаучных методов исследования, таких как анализ, синтез, логический, восхождения от абстрактного к конкретному, индукция, дедукция и др.

Результаты: определено, что развитие цифрового (кибер-) пространства и цифровых технологий способствует интенсивности терроризма, а также привело к изменению механизма совершения преступлений террористической направленности. Сделан вывод о том, что для обеспечения эффективности мер по противодействию преступлениям террористической направленности, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий, необходимы четкая стратегия и соответствующая нормативная правовая база.

Научная новизна: в работе проанализированы такие формы преступной деятельности террористических формирований, совершаемые в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, как распространение идеологии насилия и пропаганда террористической деятельности, вербовка новых членов и их обучение, применения цифровых технологий в процессе приготовительной и непосредственной террористической деятельности, финансирование.

Выявлены преимущества использования цифрового пространства и (или) цифровых технологий в процессе совершения преступлений террористической направленности. Изменение механизма совершения преступлений террористической направленности в связи с использованием цифровых технологий, по мнению автора, должно учитываться в процессе криминализации (изменении интенсивности пенализации) общественно опасных деяний. К важным направлениям государственной политики в сфере противодействия данным преступлениям отнесены воспитательно-просветительская деятельность, обучение сотрудников правоохранительных органов, расширение их полномочий для обеспечения четкого и эффективного контроля цифрового контента.

Практическая значимость: определяется возможностью использования сформулированных выводов и предложений для дальнейшей научной разработки уголовной политики государства в сфере противодействия преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

Для цитирования

Антонова, Е. Ю. (2023). Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию. *Journal of Digital Technologies and Law*, *1*(1), 251–269. https://doi.org/10.21202/jdtl.2023.10

Содержание

Введение

Преступления в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий/систем/программ представляют естественную эволюцию преступности, обусловленную научно-техническим прогрессом и новыми разработками, и относятся к числу серьезных проблем современного мира.

Не являются исключением и преступления террористической направленности. Отмечается, что уровень терроризма продолжает расти, как и «технологические достижения, способствующие привлечению внимания и эмоционального воздействия террористов» (Orehek & Vazeou-Nieuwenhuis, 2014). Исследователями фиксируется прямая связь между цифровым (кибер-) пространством и различными формами социально-политической дестабилизации: антиправительственными демонстрациями, беспорядками и террористическим актами (Khokhlov & Korotayev, 2022).

Заместитель секретаря Совета безопасности России Ю. Коков справедливо замечает, что наступает эра цифрового терроризма, который по масштабам возможных последствий может быть сопоставим с оружием массового уничтожения. По его данным, в Интернете действуют около 30 тыс. террористических и экстремистских сайтов[1]. Данные обстоятельства требуют серьезной работы по противодействию преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий/систем/программ.

1. Формы преступной деятельности террористических формирований, совершаемые в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий

Лица, вовлеченные в террористическую деятельность, активно используют современные цифровые технологии как в процессе совершения преступлений, так и в повседневной жизни. Такие технологии применяются внутри террористических сообществ/организаций (далее – формирований) в качестве инструмента коммуникации, в том числе в процессе организации и руководства террористической деятельностью, а также при вербовке новых членов террористических формирований, распространении идеологии насилия, пропаганды террористической деятельности, призывов к совершению конкретных террористических актов. Члены террористических формирований стремятся донести такие сообщения, а также продемонстрировать свои противоправные деяния максимально широкой аудитории, поскольку основной их целью является дестабилизация общества, его моральная и политическая нестабильность.

[1] СБ РФ: цифровой терроризм может быть сопоставим с оружием массового уничтожения. (2022, 18 мая). *ТАСС*. https://tass.ru/politika/14658343/amp

1.1. Распространение идеологии насилия, пропаганда террористической деятельности через цифровое (кибер-) пространство

Идеология насилия играет одну из ведущих ролей в совершении преступлений террористической направленности (Антонова, 2018). Терроризм – это политический инструмент, требующий мотивации и способностей, которые определяют его масштабы, происхождение, идеологию и контрстратегии (Orehek & Vazeou-Nieuwenhuis, 2014). Отмечается, что успех ИГИЛ* зависит в том числе от того, что группа «работает как организация хорошо подготовленных, идеологически мотивированных и безжалостных бойцов» (Makinda, 2016). Интернет стал неуправляемым цифровым пространством, используемым в том числе для распространения и культивирования идеологии терроризма.

К примеру, субъекты групп крайне правого крыла (XRW) используют Интернет для обращения в свою веру, пропаганды зверств террористов и для их максимальной огласки, транслируя свои атаки в прямом эфире. Так, из 22 террористических заговоров, раскрытых в Великобритании, в период с марта 2017 г. по сентябрь 2019 г., семь были вдохновлены идеологией XRW. В этот же период лица, вдохновленные идеологией XRW, совершили три террористических акта со смертельным исходом (Zedner, 2021). Таким образом, в цифровую эпоху можно чувствовать себя очень тесно связанным с онлайн-группами и онлайн-контактами, которые могут иметь схожие интересы и идеологию насилия (Liem et al., 2018), хотя и не быть членом этих групп, действуя в одиночку, в том числе в террористических целях.

Террористические формирования пользуются тем, что цифровое (кибер-) пространство позволяет передавать информацию мгновенно, за считаные секунды, на неопределенно широкую территорию. Через Интернет, мобильные устройства и платформы социальных сетей быстро распространяется очень возбуждающий и потенциально тревожный видеоконтент событий, в том числе в прямом эфире можно наблюдать за международными террористическими атаками, сопровождающимися взрывами и стрельбой (Huddy et al., 2021). Кроме того, по каналам социальных сетей происходит реагирование официальных властей и широкой общественности на опасные ситуации. Растущий рост использования Twitter** и Facebook*** во время чрезвычайных ситуаций является ярким свидетельством того, что общественность принимает публикуемую или размещаемую в цифровом (кибер-) пространстве информацию как «правду». Несмотря на то, что настоящее время называют эпохой фальшивых новостей или дезинформации, общественность по-прежнему в целом доверяет информации, получаемой в Интернете или социальных сетях (Grobbelaar, 2022).

Распространяя через цифровое (кибер-) пространство информацию, не всегда соответствующую действительности (это может быть и дезинформация, слухи, угрозы применения насилия или изображения актов насилия), террористические формирования оказывают воздействие не только на возможных или действительных сторонников террористических воззрений, идеологии насилия (что используется в первую очередь для вербовки новых членов, радикализации, подстрекательства к терроризму, подрыва веры в социальные ценности), но и на прямых или косвенных жертв террористических актов (устрашение населения путем психологического манипулирования, распространения чувств повышенного беспокойства, тревоги, страха или паники среди населения) или на органы власти и международное сообщество в целом (дестабилизация деятельности органов власти или международных организаций либо воздействие на принятие ими решений).

Это обусловлено и тем обстоятельством, что терроризм понимают и как преднамеренное использование или угрозу применения насилия отдельными лицами или субнациональными группами для достижения политической или социальной цели путем запугивания большой аудитории, помимо непосредственной жертвы (Sandler, 2013). Так, в период с 2014 по 2017 г. ИГИЛ* обезглавила 296 человек и опубликовала видеозаписи западных заложников, в том числе американских журналистов Джеймса Фоули и Стивена Сотлоффа, а также британских гуманитарных работников Дэвида Хейнса и Алана Хеннинга. Все четверо заложников были казнены в 2014 г. В ходе опроса HuffPost-YouGov, проведенного в ноябре 2014 г., 32 % американцев заявили, что видели, по крайней мере, несколько видеороликов с обезглавливанием ИГИЛ*, а 9 % заявили, что видели фактическое обезглавливание. Согласно данным, полученным на национальном уровне от репрезентативной онлайн-группы, опрошенной примерно через шесть-девять месяцев после самых известных казней в США, 25 % американцев заявили, что видели часть или все видео с обезглавливанием (Huddy et al., 2021). Такие действия направлены в первую очередь на устрашение населения и распространение чувства повышенной тревоги и страха, которые могут привести к панике среди населения.

Кроме того, действия террористов часто направлены на то, чтобы спровоцировать реакцию правительства, такую как территориальные уступки или политические реформы посредством актов запугивания, которые истощают решимость противостоящего правительства или подчеркивают его неэффективность (Huddy et al., 2021). Именно поэтому террористические формирования стремятся адаптировать экстремальные средства коммуникации для привлечения внимания и видимости в глобальной медиасреде. Насилие террористов, в высшей степени опосредованное и зрелищное, порождает превращение атак в медиасобытия, которые разворачиваются в гибридном пространстве и укореняются в доступных возможностях и технологиях (Uusitalo et al., 2021).

Для совершения пропагандистских действий террористические формирования задействуют широкий спектр технических средств: веб-сайты, чат-группы и чат-форумы, онлайн-журналы, платформы таких социальных сетей, как Twitter** и Facebook***, популярные видео- и файлообменные веб-сайты, например, YouTube. Поисковые системы Интернета упрощают нахождение террористического контента.

На слушаниях в подкомитете по информации и борьбе с терроризмом Комитета Национальной безопасности палаты представителей Правительства США были приведены примеры использования террористами систем искусственного интеллекта (далее – ИИ). Так, один из сторонников превосходства белой расы открыл огонь по двум мечетям в Крайстчерче (Новая Зеландия), убив 51 человека и ранив еще 49. Террорист смог транслировать нападение в прямом эфире на Facebook***, потому что ИИ этой сети не счел отснятый материал достаточно ужасным. Затем видео было 300 000 раз успешно загружено на Facebook*** другими пользователями. Это доказывает, что технологии ИИ, призванные блокировать такие видео, еще не справляются с поставленной задачей. Более того, имеются факты, свидетельствующие о том, что ИИ Facebook*** снимает видео и продвигает террористический контент, который он должен был удалить[2].

[2] Artificial Intelligence and Counterterrorism: Possibilities and Limitations. (2020). *Hearing Before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security House of Representatives One Hundred Sixteenth Congress. First Session. June 25, 2019* (Serial № 116-28). Washington: U.S. Government Publishing Office.

Но даже если преступники не транслируют атаку в прямом эфире, свидетели визуально записывают события, и эти видеоматериалы включаются в сегменты новостей, которые часто загружаются на онлайн-сайты, такие как YouTube, а также на платформы социальных сетей, такие как WhatsApp и Snapchat. Этот необработанный графический видеоконтент легкодоступен (иногда сопровождается необоснованным предупреждением) и может вызвать сильные эмоции у зрителей, потенциально усиливая общественную реакцию на акт террора (Huddy et al., 2021).

1.2. Вербовка новых членов террористических формирований и их обучение

Важную роль в деятельности террористических формирований играет вербовка новых членов, поскольку неспособность набрать достаточное количество членов и провести успешные атаки свидетельствует о слабости группы (Polo, 2020). Развитие информационных-телекоммуникационных технологий, особенно Интернета и его инструментов, обеспечивает платформу, используемую террористическими формированиями для вербовки новых членов и распространения своей пропаганды (Dingji Maza, 2020), а также для их онлайн-обучения и планирования террористических атак.

Так, использование «Аш-Шабааб» видео и сообщений через Интернет сделало эту террористическую организацию известной во всем мире. До 2009 г. «Аш-Шабааб» набирала в свои ряды исключительно сомалийцев. Однако с тех пор, как начались их публичные связи с «Аль-Каидой»*, были завербованы иностранные боевики, которые идеологически отождествляли себя с глобальным джихадом. Один из их самых известных международных бойцов Омар Хаммами, также известный как Абу Мансур аль-Амрики, начиная с 2010 г. регулярно публиковал в Интернете сообщения и распространял их как вербовка «Аш-Шабааб» (Grobbelaar, 2022).

Отмечается, что создание локальных сетей террористических формирований или присоединение к ним способствует передаче знаний и обучению; позволяет проводить совместные тренировки и планирование атак; увеличивает доступность, поставку и обмен оружия, личного состава и другого капитала, связанного с терроризмом; локальные сети даже позволяют группам создавать альянсы, объединяться и проводить скоординированные кампании против государства. Террористические сети, таким образом, действуют как решающий фактор, увеличивающий силу, поддерживая потенциал групп, их возможности и эффективность (Polo, 2020).

Кроме того, специализированные террористические сайты работают как онлайн-библиотеки идеологических текстов, платформы для вербовщиков и форумы для обмена информацией. Фото- и видеоматериалы, игры (имитирующие террористические атаки и побуждающие пользователей участвовать в ролевой игре, выступая в роли виртуального террориста), учебные пособия и технические инструкции, подготовленные террористическими группами, способствуют радикализации их сторонников (Khokhlov & Korotayev, 2022). Пропагандистские материалы могут содержать идеологические или практические руководства, разъяснения, оправдания или рекламу деятельности террористов.

Так, в ходе проверки Шахунской городской прокуратурой Нижегородской области интернет-ресурсов, осуществляемой с использованием программы браузера Google Chrome, в поисковом ресурсе «Яндекс» при введении ключевых слов: «Expedient Homemade Firearms», отобразился список интернет-сайтов, содержащий ссылки:

<данные изъяты>. На указанных интернет-страницах размещена подробная информация о способах самостоятельного изготовления оружия, проходит ее обсуждение. Доступ к материалам свободный для всех пользователей, сайт и интернет-страницы не содержат ограничений к его доступу по кругу лиц, не требуются предварительная регистрация и пароль, ознакомиться с содержанием данной интернет-страницы и скопировать материалы в электронном варианте может любой пользователь, ограничения на передачу, копирование и распространение отсутствуют[3].

Как отмечают специалисты, воздействие на компьютерную информацию позволяет преступнику «манипулировать эмоциями и сознанием потерпевшего, вызывая серьезные психофизиологические последствия. Психоэмоциональный эффект сравним по силе с эффектом от событий в реальном мире, в то же время он смоделирован путем изменения компьютерной информации» (Дремлюга, 2022).

Исследования показывают, что социальные движения часто используют цифровое медиапространство для работы с идентификацией, используя цифровые сообщения для развития здравого смысла «мы» (Gaudette et al., 2020). Собраны значительные доказательства того, что социальные медиа стали местом формирования идентичностей и способствуют формированию сообществ с сильным чувством групповой солидарности (Törnberg & Törnberg, 2022). К таким психологическим приемам и прибегают террористические формирования в процессе вербовки новых членов и пропаганды своей идеологии.

1.3. Применение цифровых технологий в процессе приготовительной и непосредственной террористической деятельности

В науке отмечаются феноменальные успехи систем ИИ не только в области цифровых платформ, но и в материальной, непосредственной среде. Это напрямую видно на примере внедрения цифровых технологий (современной робототехники) в систему беспилотного управления транспортных средств, что облегчает совершение террористических актов. Уже на практике встречаются случаи применения цифровых технологий, в том числе беспилотников, в процессе приготовительной и непосредственной террористической деятельности, в частности для доставки наркотиков, психоактивных веществ и других запрещенных предметов – оружия, взрывчатых веществ, взрывных устройств и пр.

Так, террористические группы все чаще используют беспилотники для наблюдения, взрывов и других общественно опасных действий как на стадии приготовления, так и непосредственного совершения актов терроризма. Сообщается, что ИГИЛ* начала использовать боевые дроны в Ираке и объявила о создании подразделения «Беспилотные летательные аппараты моджахедов»[4]. Кроме того, ИГИЛ* провела несколько бомбардировок с использованием беспилотников, нацеленных

---

[3] Архив Шахунского районного суда Нижегородской области. Решение № 2А-214/2021 от 22 марта 2021 г. Дело № 2А-214/2021. (2021). *Судебные и нормативные акты РФ*. https://sudact.ru/regular/doc/AAQ1OEJsQbb9/

[4] Joby, Warrick. (2017, February 17). Use of weaponized drones by ISIS spurs terrorism fears. *The Washington Post*. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html

как на гражданские, так и на военные цели, и даже предпринимала попытки атаковать беспилотниками глав государств[5]. По мере увеличения производства этих гаджетов и снижения себестоимости эти новшества станут более привлекательными и полезными для отдельных террористов и террористических формирований. Ножи и грузовики все еще могут быть более простыми и дешевыми вариантами, но новые методы террористической атаки начнут реализовываться[6].

3D-принтеры также могут сделать сложные и дорогие технологии доступными для террористов. Так, напавший на немецкую синагогу в Йом-Кипур в начале октября 2019 г. использовал напечатанные на 3D-принтере компоненты самодельного оружия[7]. В 2020 г. немецкий террорист потратил всего 50 долларов на 3D-печать деталей для оружия, которое использовалось при попытке нападения в Галле[8].

Цифровое (кибер-) пространство используется и в качестве средства для совершения кибератак, призванных нарушить нормальное функционирование компьютерных систем, серверов с помощью компьютерных вирусов, вредоносных и шпионских программ или других средств неправомерного доступа к компьютерной информации. Этим действиям характерны такие черты террористического акта, как стремление путем устрашения населения способствовать дестабилизации деятельности органов власти или международных организаций, воздействовать на принятие ими решений и таким образом достичь политических или иных социальных целей.

1.4. Цифровые каналы финансирования терроризма

Для достижения поставленных целей и эффективной деятельности террористические формирования привлекают значительные материальные (финансовые) ресурсы. Цифровое (кибер-) пространство и новые цифровые технологии только способствуют быстрому получению доходов, которые в последующем используются для нужд террористов.

Различные исследования показывают, что террористические группы, такие как «Аль-Каида»*, «Хамас» и моджахеды, получают финансирование и поддержку посредством цифровых платежей от групп и отдельных лиц, симпатизирующих их делу. Примеры таких цифровых платежей включают интернет-банкинг, мобильный перевод средств, онлайн-торговлю и более широкое использование криптовалют, таких как биткоин (Dingji Maza et al., 2020). Руководитель Антитеррористического центра СНГ А. Новиков отмечает, что «произошла цифровая трансформация механизмов и каналов финансирования терроризма». В качестве источников доходов террористы используют онлайн-казино, прибегают к хищениям денежных средств через подставные интернет-магазины и сайты-двойники, используют фишинговые и фарминг-атаки, несанкционированный доступ к банковским ресурсам и криптовалютным биржам[9].

---

5 Gavin, J. *Trends in Terrorism [2022].* Vision of Humanity. https://www.visionofhumanity.org/trends-in-terrorism/

6 Noor, E. (2020, January 29). *Sharing space: Tech and terrorism.* Observer Research Foundation. https://www.orfonline.org/expert-speak/sharing-space-tech-terrorism-60862/

7 Beau Jackson. (2019, October 18). "Interview with the ICSR: A 3D printed gun was not used in the Halle terror attack". *3D Printing Industry*. https://3dprintingindustry.com/news/interview-with-the-icsr-a-3d-printed-gun-was-not-used-in-the-halle-terrorattack-163643/

8 Gavin, J. *Trends in Terrorism [2022]*. Vision of Humanity. https://www.visionofhumanity.org/trends-in-terrorism/

9 *Террористы все активнее используют IT-технологии, заявили в АТЦ СНГ*. (2020, 3 марта). РИА Новости. https://ria.ru/amp/20200218/1564913906.html

Кроме того, через цифровое (кибер-) пространство террористические формирования обращаются с прямыми просьбами о пожертвованиях. Для этого используются веб-сайты, чат-группы, массовые рассылки сообщений с просьбами о пожертвованиях.

Так, Северо-Кавказский окружной военный суд вынес обвинительный приговор в отношении Ш., который опубликовал в Интернете призыв к сбору денежных средств на нужды ИГ*. Полученные деньги он перевел на счет террористической группировки[10]. В другом случае следствием и судом установлено, что М. перечислил через платежный терминал 7 000 руб. на счет электронного кошелька, который использовался для сбора денежных средств с целью оказания финансовой помощи членам группировки «Хайят Тахрир аш-Шам»*, являющейся структурным подразделением запрещенной террористической организации «Джебхат ан-Нусра»*[11].

Веб-сайты используются и в качестве интернет-магазинов, предлагающих книги, аудио-, видеозаписи и иные материалы с соответствующим содержанием. Продажа такого товара позволяет не только получить дополнительный доход, но и способствует распространению идеологии терроризма.

2. Преимущества использования цифрового пространства и (или) цифровых технологий в процессе совершения преступлений террористической направленности

Преимущества использования цифрового пространства и (или) цифровых технологий обусловлены, во-первых, скоростью передачи данных и распространения информации (дезинформации), а также обработки большого массива информации, позволяющей, например, оперативно отыскивать сторонников, вербовать новых членов террористических формирований и т. д.; во-вторых, охватом неопределенно широкой аудитории и расширением географии распространения деструктивной идеологии насилия в условиях относительной анонимности; в-третьих, сложностью контролирования содержательной части распространяемой информации; в-четвертых, упрощением координации действий членов террористических формирований.

Кроме того, к очевидным преимуществам цифровых технологий относят возможность их использования на любых, в том числе представляющих опасность территориях (зоны военных конфликтов); физическую безопасность субъектов, их применяющих (при использовании опасных предметов – химических, отравляющих или взрывчатых веществ и др.), и сложность их обнаружения (Антонова, 2022).

Перечисленные и иные факторы во многих случаях увеличивают степень общественной опасности совершаемых деяний, что должно быть отражено и в нормах уголовного закона.

---

[10] *В Дагестане суд приговорил собиравшего средства для ИГ мужчину к 17 годам* (2019, 2 августа). РБК. https://www.rbc.ru/rbcfreenews/5d44544c9a7947190c12566e

[11] *В Российской Федерации вынесен приговор за финансирование терроризма*. (2020, 30 сентября). Eurasian Group. URL: https://eurasiangroup.org/ru/sentence-for-terrorist-financing-in-russian-federation34

Особо привлекательной для террористических формирований в этом плане является несовершеннолетняя аудитория, поскольку она не имеет необходимого жизненного опыта, устойчивых положительных ориентаций и является активным пользователем цифрового (кибер-) пространства. К тому же как отмечается в научной литературе, «подростки подвержены формированию установок на агрессивное поведение». Наиболее действенными в отношении них являются технологии разжигания агрессии посредством экстремистских лозунгов, политизации социально-экономических проблем, романтизации образов «отрицательных героев», навязывания идей, пропагандирующих насилие как социальную норму и погружения их в деструктивные интернет-сообщества (Щетинина, 2018). Для вербовки несовершеннолетних применяются популярные музыкальные видеоролики, компьютерные игры, мультипликационные фильмы, рассказы, поощряющие и прославляющие действия террористов, миссии террористов-смертников и др.

Так, трое 15-летних подростков с октября 2019 г. по июнь 2020 г. «путем общения в одной из социальных сетей и мессенджерах, придерживаясь идей анархизма… объединились в группу для последующего совместного осуществления террористической деятельности на территории города Канска». Распределив между собой роли, подростки самостоятельно проходили обучение путем чтения запрещенной, признанной решением суда экстремистской литературы и просмотра видеофильмов по изготовлению взрывчатых веществ и взрывных устройств в целях осуществления террористической деятельности. Они самостоятельно изготавливали взрывчатые вещества и взрывные устройства и отрабатывали их применение на практике в заброшенном доме, на пустырях и стройках с целью подготовки к совершению террористического акта путем подрыва здания полиции или Управления Федеральной службы безопасности (далее – ФСБ). В материалах дела фигурировали скриншоты переписок в социальных сетях, в которых фигуранты дела обсуждали, где и как приобрести компоненты взрывчатки. Кроме того, школьники намеревались «для наглядности» построить в игре Minecraft здание ФСБ и взорвать его[12].

Все вышесказанное подтверждается и специалистами в области противодействия терроризму. Так, директор Контртеррористического управления Организации Объединенных Наций В. Воронков отмечает, что террористы активно пользуются различными технологическими достижениями. Используя социальные сети, зашифрованные сообщения («даркнет»), они распространяют свою человеконенавистническую идеологию, собирают и переводят средства, радикализуют молодежь и вербуют новых сторонников, координируют теракты. Причем они задействуют алгоритмы социальных сетей так, чтобы как можно быстрее и шире распространять свой контент. Есть данные о попытках террористического подполья использовать лекарственные препараты для создания биологического оружия. Для доставки химических, биологических или радиологических материалов террористы могут применять беспилотники, в том числе автоматические[13].

---

12 *Подростка из Канска приговорили к 5 годам колонии за подготовку теракта*. (2022, 10 февраля). Деловой Петербург. https://www.dp.ru/a/2022/02/10/Podrostka_iz_Kanska_prigo

13 *В Минске обсуждают возможности новых технологий и искусственного интеллекта в борьбе с терроризмом.* (2019, 3 сентября). Организация Объединенных Наций. https://news.un.org/ru/story/2019/09/1362292

3. Противодействие преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий

Сложность противодействия цифровой преступности в первую очередь обусловлена тем, что она «не поддается внятному количественному измерению; объяснение этому имеет комплексный характер: противоречия действующего нормативного регулирования, несовершенство правоприменительной деятельности и механизмов статистического учета… бесчисленность и постоянно видоизменяющаяся природа цифровой преступности» (Русскевич и др., 2022).

Для противодействия преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, требуется выработка эффективных механизмов, в том числе уголовно-правового воздействия, которые позволят своевременно реагировать на террористические угрозы в цифровой среде.

Отметим, что сложность противодействия общественно опасным деяниям, в том числе террористической направленности, совершаемым в цифровом пространстве, как правило, приводит к изменениям в нормативных правовых базах государств. Чаще всего такие изменения связаны с усилением правовой ответственности за совершение подобных деяний.

Так, в связи с тем, что виновными в терроризме часто являются субъекты-одиночки, радикализирующиеся в Интернете, в Разделе 3 Закона Великобритании о борьбе с терроризмом и безопасности границ (CTBSA) 2019 г. установлена уголовная ответственность за однократный просмотр в Сети «материалов, которые могут быть полезны лицу, совершающему или готовящему террористический акт». Такое деяние влечет назначение максимального наказания в виде 15 лет лишения свободы (Zedner, 2021).

В российское уголовное законодательство также вносятся изменения: нормы дополняются квалифицирующим (особо квалифицирующим) признаком «совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет», видоизменяются и появляются новые нормы о преступлениях в сфере компьютерной информации. Несмотря на все законодательные нововведения констатировать наличие должной, эффективной системы мер уголовно-правового воздействия на лиц, совершающих рассматриваемые деяния в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, пока нельзя. Анализ норм уголовного закона показывает, что к настоящему времени российский законодатель усилил лишь ответственность за публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганду терроризма (ст. 2052), в случае их совершения в цифровом (кибер-) пространстве (ч. 2). Во всех остальных нормах о преступлениях террористической направленности соответствующий квалифицирующий (особо квалифицирующий) признак отсутствует. Вместе с тем практика показывает, что цифровое (кибер-) пространство используется не только для распространения пропагандистской информации в террористических целях, но и для содействия террористической деятельности, включая вербовку новых членов террористических формирований, финансирование, обучение исполнителей, подстрекательство к совершению террористических актов и др.

Следует иметь в виду, что противодействовать преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или)

с использованием цифровых технологий, только путем криминализации новых общественно опасных деяний или усиления интенсивности пенализации невозможно. Необходимо четкое понимание механизма совершения таких преступлений. Отсюда новые задачи стоят и перед правоохранительными органами, которые должны уметь оперативно выявлять источник террористической угрозы и блокировать/ликвидировать его.

К тому же, как отмечается в научной литературе, быстрое развитие цифровых технологий, интеллектуальных устройств и социальных сетей ухудшило способность сотрудников служб общественной безопасности управлять общественным реагированием на террористическую атаку. Поскольку люди (спецслужбы) все больше полагаются на цифровые технологии, неизвестно как они начнут действовать в случае сбоя киберсистем. В связи с этим возрастает вероятность каскадной катастрофы и возникновения киберуязвимости (Keenan, 2019). Все это может быть использовано террористическими формированиями и должно учитываться при выработке мер по противодействию таким преступлениям.

Выводы

Проведенный анализ различных форм преступной деятельности террористических формирований, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, позволяет констатировать, что:

1) развитие цифрового (кибер-) пространства (социальных сетей, электронных СМИ и других интернет-ресурсов), увеличение числа пользователей таким пространством и цифровыми технологиями/системами/программами способствуют расширению идеологии насилия за счет активной пропагандистской деятельности террористических формирований и, как результат, интенсивности терроризма;

2) использование цифровых технологий террористическими формированиями, по сути, ведет к изменению механизма совершения преступлений террористической направленности – от стадии приготовления до оконченного преступления и сокрытия его следов.

Данные обстоятельства должны быть учтены и при выработке конструктивных, эффективных мер по противодействию преступлениям террористической направленности. Современные цифровые технологии необходимо активнее использовать в процессе выявления, раскрытия и расследования преступлений террористической направленности, особенно когда таковые совершаются в цифровом (кибер-) пространстве, а также с использованием IT-технологий. Важным аспектом в этой связи является возможность использования ИИ оперативно-разыскными подразделениями (например, система распознавания лиц, идентификация личности, номеров транспортных средств, мониторинг социальных сетей и т. д.).

Цифровое (кибер-) пространство может эффективно быть использовано для проведения оперативно-разведывательных действий, сбора информации, извлекаемой из сообщений на веб-сайтах, в чатах и других цифровых ресурсах, что будет способствовать своевременному предотвращению и пресечению террористических актов, сбору доказательственной базы для привлечения субъектов террористической деятельности к уголовной ответственности.

Еще одной контрмерой является создание веб-сайтов, чат-групп, чат-форумов и других интернет-платформ для ведения конструктивных онлайн-дискуссий, демонстрации контртеррористических и иных воспитательно-просветительских материалов, опирающихся на конкретные факты, изложения альтернативных ненасильственных методов решения политических и иных социальных проблем.

Для эффективного выявления, раскрытия и расследования преступлений террористической направленности, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, сотрудники правоохранительных органов должны обладать не только правовыми, но и специальными техническими знаниями по механизму совершения данных преступлений. Они должны знать современные цифровые (компьютерные, информационно-коммуникационные) технологии/системы/программы, механизм и порядок их работы.

Таким образом, для обеспечения эффективности мер по противодействию преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, необходима четкая стратегия и соответствующая нормативная правовая база, которые должны быть нацелены:

1) на криминализацию (изменение интенсивности пенализации) общественно опасных деяний (в том числе террористической направленности), совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий. Для этого необходима ревизия уголовного закона и иных нормативных правовых актов в сфере цифровых технологий в целях выявления пробелов правовой защиты объектов от террористических угроз и определения потребности усиления ответственности в конкретных случаях. Допускаем, что совершение преступлений в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий не во всех случаях может увеличивать степень общественной опасности запрещенных деяний. В этой связи на современном этапе считаем достаточным дополнить ст. 63 УК РФ частью 12 и изложить ее в следующей редакции «12. Судья (суд), назначающий наказание, в зависимости от характера и степени общественной опасности преступления, обстоятельств его совершения и личности виновного может признать отягчающим обстоятельством совершение преступления с использованием цифровых и информационно-телекоммуникационных технологий»;

2) усиление сил и средств на воспитательно-просветительскую деятельность, в том числе в цифровом (кибер-) пространстве, направленную на пропаганду «мирного сосуществования всех народов независимо от расы, национальности, языка, происхождения в противовес негативному информационно-идеологическому воздействию на личность извне, в том числе пропаганды идеологии терроризма» (Ищук и др., 2021);

3) обучение сотрудников правоохранительных органов, выявляющих, раскрывающих и расследующих преступления, в том числе террористической направленности, совершаемые в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий;

4) расширение полномочий сотрудников правоохранительных органов для обеспечения четкого и эффективного контроля цифрового контента;

5) выработку соглашений по международному сотрудничеству в области противодействия преступлениям, в том числе террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

---

* Организация признана террористической, ее деятельность запрещена на территории Российской Федерации.

** Социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.

*** Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

Список литературы

Антонова, Е. Ю. (2018). Терроризм как идеология насилия. *Вестник Дальневосточного юридического института МВД России*, *2*(43), 69–74. https://elibrary.ru/usgvtk

Антонова, Е. Ю. (2022). Технологии искусственного интеллекта – субъект преступления или орудие/средство совершения преступления? *Юридический вестник Кубанского государственного университета*, *1*, 31–39. EDN: https://elibrary.ru/liybhv. DOI: https://doi.org/10.31429/20785836-14-1-31-39

Дремлюга, Р. И. (2022). *Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение*: монография. Москва: Юрлитинформ. https://elibrary.ru/hsbxrm

Ищук, Я. Г., Пинкевич, Т. В., Смольянинов, Е. С. (2021). *Цифровая криминология*: учебное пособие. Москва: Академия управления МВД России. https://elibrary.ru/vckoef

Русскевич, Е. А., Дмитренко, А. П., Кадников, Н. Г. (2022). Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации. *Вестник Санкт-Петербургского университета. Право*, *13*(3), 585–598. EDN: https://elibrary.ru/xlyjys. DOI: https://doi.org/10.21638/spbu14.2022.301

Щетинина, Е. В. (2018). Проблемы развития культуры насилия в интернет-пространстве. *Инновационное развитие профессионального образования*, *18*(2), 127–130. https://elibrary.ru/xrzrml

Dingji Maza, K., Koldaş, U., & Aksit, S. (2020). Challenges of Combating Terrorist Financing in the Lake Chad Region: A Case of Boko Haram. *SAGE Open*, *10*(2), 215824402093449. https://doi.org/10.1177/2158244020934494

Gaudette, T., Scrivens, R., & Venkatesh, V. (2020). The role of the internet in facilitating violent extremism: insights from former right-wing extremists. *Terrorism and Political Violence*. Epub ahead of print 16 July.

Grobbelaar, A. (2022). Media and Terrorism in Africa: Al-Shabaab's Evolution from Militant Group to Media Mogul. *Insight on Africa*, *15*(1), 7–22. https://doi.org/10.1177/09750878221114375

Huddy, L., Smirnov, O., Snider, K. L. G., & Perliger, A. (2021). Anger, Anxiety, and Selective Exposure to Terrorist Violence. *Journal of Conflict Resolution*, *65*(10), 1764–1790. https://doi.org/10.1177/00220027211014937

Keenan, P. K. (2019). Creating spaces of public insecurity in times of terror: The implications of code/space for urban vulnerability analyses. *Environment and Planning C: Politics and Space*, *37*(1), 81–101. https://doi.org/10.1177/2399654418776660

Khokhlov, N., & Korotayev, A. (2022). Internet, Political Regime and Terrorism: A Quantitative Analysis. *Cross-Cultural Research*, *56*(4), 385–418. https://doi.org/10.1177/10693971221085343

Liem, M., van Buuren, J., de Roy van Zuijdewijn, J., Schönberger, H., & Bakker, E. (2018). European Lone Actor Terrorists Versus "Common" Homicide Offenders: An Empirical Analysis. *Homicide Studies*, *22*(1), 45–69. https://doi.org/10.1177/1088767917736797

Makinda, S. (2016). Terrorism in International Society: An Eclectic Perspective. *Journal of Asian Security and International Affairs*, *3*(1), 90–101. DOI: https://doi.org/10.1177/2347797015626053

Orehek, E., & Vazeou-Nieuwenhuis, A. (2014). Understanding the Terrorist Threat: Policy Implications of a Motivational Account of Terrorism. *Policy Insights From the Behavioral and Brain Sciences*, *1*(1), 248–255. https://doi.org/10.1177/2372732214549747

Polo, S. M. T. (2020). How Terrorism Spreads: Emulation and the Diffusion of Ethnic and Ethnoreligious Terrorism. *Journal of Conflict Resolution*, *64*(10), 1916–1942. https://doi.org/10.1177/0022002720930811

Sandler, T. (2013). The analytical study of terrorism. *Journal of Peace Research*, *51*(2), 257–271. https://doi.org/10.1177/0022343313491277

Törnberg, P., & Törnberg, A. (2022). Inside a White Power echo chamber: Why fringe digital spaces are polarizing politics. *New Media & Amp; Society*, 146144482211229. https://doi.org/10.1177/14614448221122915

Uusitalo, N., Valaskivi, K., & Sumiala, J. (2021). Epistemic modes in news production: How journalists manage ways of knowing in hybrid media events involving terrorist violence. *Journalism*, *23*(9), 1811–1827. https://doi.org/10.1177/14648849211015601

Zedner, L. (2021). Countering terrorism or criminalizing curiosity? The troubled history of UK responses to right-wing and other extremism. *Common Law World Review*, *50*(1), 57–75. https://doi.org/10.1177/1473779521989349

Сведения об авторе

Антонова Елена Юрьевна – доктор юридических наук, профессор, декан юридического факультета, Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации
Адрес: 690091, Российская Федерация, г. Владивосток, ул. Суханова, 8
E-mail: antonovy@yandex.ru
ORCID ID: https://orcid.org/0000-0001-6605-3699
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/rid/ABD-6781-2021
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57205298413
Google Scholar ID: https://scholar.google.com/citations?user=dqfYMLYAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=261147

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 24 октября 2022 г.
Дата одобрения после рецензирования – 6 декабря 2022 г.
Дата принятия к опубликованию – 6 марта 2023 г.
Дата онлайн-размещения – 10 марта 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.10

Terrorist Crimes in the Era of Digitalization: Forms of Activity and Measures for Counteraction

Elena Yu. Antonova

Far East Juridical Institute (branch) of the University of Public Prosecution of the Russian Federation
Vladivostok, Russian Federation

Keywords

Counteraction,
crime,
criminalization,
digital funding,
law,
propaganda,
recruitment,
space,
technologies,
terrorism

Abstract

Objective: to elaborate recommendations on counteraction against terrorist crimes committed in the digital (cyber-) space and/or using digital technologies.

Methods: the methodological basis of the research are the universal dialectic method of cognition, the integrity of general and specific scientific methods such as analysis, synthesis, logical method, ascent from the abstract to the specific, induction, deduction, etc.

Results: it was determined that the development of the digital (cyber-) space and digital technologies promotes the intensity of terrorism and has led to the change of the mechanism of terrorist crimes commitment. A conclusion was made that, to provide the efficiency of measures for counteracting terrorist crimes committed in the digital (cyber-) space and/or using digital technologies, a distinct strategy is necessary, as well as the appropriate regulatory basis.

Scientific novelty: the article analyzes such forms of criminal activities of terrorist groups, committed in the digital (cyber-) space and/or using digital technologies, as dissemination of the ideology of violence and propaganda of terrorist activity, recruiting new members and their training, implementing digital technologies for preparation and immediate terrorist activity, and funding. The advantages were revealed of the use of digital space and/or digital technologies when committing terrorist crimes. In the author's opinion, the change of the mechanism of terrorist crimes commitment associated with the use of digital technologies should be taken into account during criminalization (change of the intensity of penalization) of publicly dangerous deeds. The important areas of state policy in the sphere of counteraction against these crimes are education and enlightenment activity, training of the personnel of law-enforcement agencies, broadening their authorities to ensure a clear and effective control over digital content.

Practical significance: is due to the possibility to use the formulated conclusions and proposals for further scientific elaboration of the state criminal policy in the sphere of counteraction against terrorist crimes committed in the digital (cyber-) space and/or using digital technologies.

For citation

Antonova, E. Yu. (2023). Terrorist Crimes in the Era of Digitalization: Forms of Activity and Measures for Counteraction. *Journal of Digital Technologies and Law, 1*(1), 251–269. https://doi.org/10.21202/jdtl.2023.10

References

Antonova, E. Yu. (2018). Terrorism as the ideology of violence. *Vestnik Dalnevostochnogo yuridicheskogo instituta MVD Rossii*, *2*(43), 69–74. (In Russ.).

Antonova, E. Yu. (2022). Technologies of artificial intelligence – a subject or a tool/means of crime? *Yuridicheskiy vestnik Kubanskogo gosudarstvennogo universiteta*, *1*, 31–39. https://doi.org/10.31429/20785836-14-1-31-39

Dingji Maza, K., Koldaş, U., & Aksit, S. (2020). Challenges of Combating Terrorist Financing in the Lake Chad Region: A Case of Boko Haram. *SAGEOpen*, *10*(2), 215824402093449. https://doi.org/10.1177/2158244020934494

Dremlyuga, R. I. (2022). *Criminal-legal protection of digital economy and informational society against cyber-criminal infringements: doctrine, law, and law enforcement*. Moscow: Yurlitinform. (In Russ.).

Gaudette, T., Scrivens, R., & Venkatesh, V. (2020). The role of the internet in facilitating violent extremism: insights from former right-wing extremists. *Terrorism and Political Violence*. Epub ahead of print 16 July.

Grobbelaar, A. (2022). Media and Terrorism in Africa: Al-Shabaab's Evolution from Militant Group to Media Mogul. *Insight on Africa*, *15*(1), 7–22. https://doi.org/10.1177/09750878221114375

Huddy, L., Smirnov, O., Snider, K. L. G. & Perliger, A. (2021). Anger, Anxiety, and Selective Exposure to Terrorist Violence. *Journal of Conflict Resolution*, *65*(10), 1764–1790. https://doi.org/10.1177/00220027211014937

Ishchuk, Ya. G., Pinkevich, T. V., & Smolyaninov, E. S. (2021). *Digital criminology*: tutorial. Moscow: Akademiya upravleniya MVD Rossii. (In Russ.).

Keenan, P. K. (2019). Creating spaces of public insecurity in times of terror: The implications of code/space for urban vulnerability analyses. *Environment and Planning C: Politics and Space*, *37*(1), 81–101. https://doi.org/10.1177/2399654418776660

Khokhlov, N., & Korotayev, A. (2022). Internet, Political Regime and Terrorism: A Quantitative Analysis. *Cross-Cultural Research*, *56*(4), 385–418. https://doi.org/10.1177/10693971221085343

Kraidy, M. (2018). Terror, territoriality, temporality: Hypermedia events in the age of Islamic state. *Television and New Media, 19*(2), 170–176.

Kydd, Andrew H., Walter, & Barbara F. (2006). The Strategies of Terrorism. *International Security*, *31*(1), 49–80.

Liem, M., van Buuren, J., de Roy van Zuijdewijn, J., Schönberger, H. & Bakker, E. (2018). European Lone Actor Terrorists Versus "Common" Homicide Offenders: An Empirical Analysis. *Homicide Studies*, *22*(1), 45–69. https://doi.org/10.1177/1088767917736797

Makinda, S. (2016). Terrorism in International Society: An Eclectic Perspective. *Journal of Asian Security and International Affairs*, *3*(1), 90–101. https://doi.org/10.1177/2347797015626053

Nossek, H. (2008). 'News media'-media events: Terrorist acts as media events. *Communications*, *33*(3), 313–330.

Orehek, E., & Vazeou-Nieuwenhuis, A. (2014). Understanding the Terrorist Threat: Policy Implications of a Motivational Account of Terrorism: Policy Implications of a Motivational Account of Terrorism. *Policy Insights From the Behavioral and Brain Sciences*, *1*(1), 248–255. https://doi.org/10.1177/2372732214549747

Polo, S. M. T. (2020). How Terrorism Spreads: Emulation and the Diffusion of Ethnic and Ethnoreligious Terrorism. *Journal of Conflict Resolution, 64*(10), 1916–1942. https://doi.org/10.1177/0022002720930811

Russkevich, E. A., Dmitrenko, A. P., & Kadnikov, N. G. (2022). Crisis and palingenesis (re-birth) of criminal law under digitalization. *Vestnik Sankt-Peterburgskogo universiteta*. *Pravo*, *13*(3), 585–598. (In Russ.). https://doi.org/10.21638/spbu14.2022.301

Sandler, T. (2013). The analytical study of terrorism. *Journal of Peace Research, 51*(2), 257–271. https://doi.org/10.1177/0022343313491277

Schwartz, Carly. (2014, November 11). Majority of Americans Think Watching ISIS Beheadings Is Disrespectful to the Victims. *Huffpost*. https://www.huffingtonpost.com.au/entry/isis-beheading-videos_n_6194498

Shchetinina, E. V. (2018). Problems of development of the culture of violence in the Internet space. *Innovatsionnoe razvitie professionalnogo obrazovaniya*, *18*(2), 127–130. (In Russ.).

Törnberg, P., & Törnberg, A. (2022). Inside a White Power echo chamber: Why fringe digital spaces are polarizing politics. *NewMedia & Amp; Society*, 146144482211229. https://doi.org/10.1177/14614448221122915

Uusitalo, N., Valaskivi, K., & Sumiala, J. (2021). Epistemic modes in news production: How journalists manage ways of knowing in hybrid media events involving terrorist violence. *Journalism*, *23*(9), 1811–1827. https://doi.org/10.1177/14648849211015601

Zedner, L. (2021). Countering terrorism or criminalizing curiosity? The troubled history of UK responses to right-wing and other extremism. *Common Law World Review*, *50*(1), 57–75. https://doi.org/10.1177/1473779521989349

Author information

Elena Yu. Antonova – Doctor of Law, Professor, Dean of Law Faculty, Far East Juridical Institute (branch) of the University of Public Prosecution of the Russian Federation
Address: 8 Sukhanov Str., 690091 Vladivostok, Russian Federation
E-mail: antonovy@yandex.ru
ORCID ID: https://orcid.org/0000-0001-6605-3699
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/rid/ABD-6781-2021
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57205298413
Google Scholar ID: https://scholar.google.com/citations?user=dqfYMLYAAAAJ
RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=261147

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – October 24, 2022
Date of approval – December 6, 2022
Date of acceptance – March 6, 2023
Date of online placement – March 10, 2023