УДК 341

СОВРЕМЕННЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО СОТРУДНИЧЕСТВА ГОСУДАРСТВ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ

А.А. Рипинская

Национальный центр законодательства и правовых исследований Республики Беларусь,
ул. Берсона 1а, г. Минск, 220030, Беларусь

Развитие высоких технологий создает угрозу совершения кибертерроризма, который по своему характеру и способу совершения может нанести вред масштабнее, чем терроризм с использованием оружия либо взрывных устройств. Настоящая статья направлена на выявление проблемных аспектов противодействия использованию информационных технологий для совершения террористических актов. В статье разработаны рекомендации по осуществлению эффективного противодействия кибертерроризму.

Ключевые слова: терроризм, кибертерроризм, международное право, права человека.

CONTEMPORARY PROBLEMS OF INTERNATIONAL LEGAL COOPERATION OF STATES IN THE FIELD OF COUNTERING CYBERTERRORISM

A.A. Ripinskaya

National Center for Legislation and Legal Research of the Republic of Belarus,
1a Bersona street, Minsk, 220030, Belarus

The development of high technologies creates a threat of cyberterrorism, which, by its nature and method of commission, can cause harm on a larger scale than terrorism using weapons or explosive devices. This article is aimed at identifying the problematic aspects of countering the use of information technology to commit terrorist acts. The article developed recommendations for the implementation of effective counteraction to cyberterrorism.

Keywords: terrorism, cyberterrorism, international law, human rights.

Терроризм и его последствия являются одним из наиболее опасных вызовов современности. Сегодня ни одно государство полностью не ограждено и не защищено от угрозы совершения на его территории актов терроризма, поэтому одной из основных задач, стоящих перед каждым

государством и международным сообществом, является противодействие терроризму.

Генеральный секретарь ООН Антониу Гутерриш справедливо указал, что борьба с терроризмом перешла в виртуальное пространство и социальные сети, зашифрованные сообщения и черный интернет активно используются для распространения пропаганды, вербовки «новобранцев» и координации преступлений [1]. На современном этапе с помощью информационных технологий осуществляется, в том числе, финансирование террористической деятельности (S/RES/2462 (2019) [2], подстрекательство к совершению террористических актов (S/RES/1624 (2005) [3]), распространение террористической идеологии (S/RES/2354 (2017) [4]) и вербовка в террористические организации (S/RES/2462 (2019) [2], [5]). Вместе с тем кибертерроризм, безусловно, носящий трансграничный характер, приводит к ухудшению и нарушению дипломатических и экономических отношений между государствами. Кибертерроризм является серьезной угрозой для банковской, транспортной и энергетической систем государств и особенно для государств, в которых правительство, государственный и частный сектора экономики функционируют с помощью информационных сетей и доступа к высоким технологиям [6, с. 42].

Международно-правовое регулирование противодействия терроризму в науке международного права становилось предметом многочисленных исследований. Непосредственно вопросы кибертерроризма и связанных с ним аспектов ранее находили свое отражение в трудах Е. А. Антонян [7], В. А. Голубева [8], Е. Ф. Довгань [9; 10; 11], Н. О. Мороз [12], У. Тафойи [13]. Одновременно с этим большинство исследований направлены на изучение вопроса статуса кибератак, криминализации актов кибертерроризма, при этом не фокусируясь на проблемах, осложняющих противодействие кибертерроризму. Настоящее исследование представляет собой комплексный анализ, направленный на выявление факторов, затрудняющих эффективную деятельность по борьбе с кибертерроризмом.

Международно-правовое сотрудничество государств в области борьбы с терроризмом развивается во многих направлениях. Основной упор делается на предупреждение возникновения и распространения терроризма, пресечение терроризма, ликвидацию последствий террористических актов, привлечение виновных в совершении терроризма лиц к ответственности. При этом, несмотря на обширную сферу взаимодействия, противодействие кибертерроризму осложняется многочисленными факторами и вопросы международного правового сотрудничества государств в борьбе с кибертерроризмом в настоящее время на универсальном уровне не урегулированы [12, с. 80].

Отсутствие определения термина «кибертерроризм». Как и в случае с термином «терроризм» «кибертерроризм» также не нашел своего единого отражения в универсальных соглашениях. Вместе с тем существующие доктринальные взгляды позволяют очертить исследуемое понятие. Так, например, В. А. Голубев и Т. А. Сайтарлы под «кибертерроризмом» понимают «преднамеренную, мотивированную атаку на информацию, обрабатываемую компьютером, компьютерную систему и сети, которая создает опасность для жизни или здоровья людей или наступление других тяжких последствий, если такие действия были содеянные с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта» [14]. Дж. Льюис определяет понятие «кибертерроризм» как «использование компьютерных сетевых инструментов для прекращения функционирования критических объектов национальной инфраструктуры (в частности, энергетических, транспортных, правительственных), либо для принуждения или устрашения правительства или гражданского населения» [15, с. 1]. У. Тафойа указывает, что «кибертерроризм – это запугивание населения посредством использования высоких технологий для достижения политических, религиозных или идеологических целей, а также действия, приводящие к отключению или удалению данных или информации о критической инфраструктуре» [13]. Д. Дэннинг определяет исследуемое понятие как «политически мотивированные хакерские операции, направленные на причинение серьезного вреда, такого как гибель людей или серьезный экономический ущерб» [16]. Вышерассмотренные определения позволяют выделить характерные для кибертерроризма признаки, в частности, использование для атак компьютерных систем и сетей с целью нарушения общественной опасности, запугивания гражданского населения, причинения ущерба и вреда критическим объектам инфраструктуры государства.

Управление ООН по наркотикам и преступности (далее – УНП ООН) отмечает, что сегодня кибертерроризм рассматривается как «киберзависимое» преступление, совершаемое в политических целях для причинения вреда критической инфраструктуре, однако такое толкование кибертерроризма, ограничивающееся только киберпреступлениями, совершаемыми в отношении критически важной инфраструктуры, не получило широкого распространения при обсуждении. УНП ООН также справедливо указывает, что неоправданное отнесение каких-либо действий к кибертерроризму может иметь пагубные последствия и привести к вынесению несоразмерных мер наказания в отношении лиц, преследуемых за совершение таких преступлений [17]. Одновременно представляется необходимым рассмотреть современные формы совершения преступлений в информационном пространстве, такие, например, как массовые рассылки о минировании объектов. Отмечается, что в последнее время получил распространение такой

способ совершения преступлений как «сваттинг», под которым рассматривают тактику, направленную на введение спецслужб в заблуждение [18]. В Российской Федерации в феврале 2022 г. были задержаны члены «сваттинговых» интернет-групп, которые оставляли ложные сообщения о минировании зданий в РФ, Беларуси, Азербайджане, Армении, Казахстане, Молдавии. Федеральная служба безопасности РФ отметила, что авторы ложных сообщений о минировании занимались этим «в целях дестабилизации обстановки в Российской Федерации и сопредельных государствах, вымогательства денежных средств из хулиганских побуждений» [19].

Сегодня все чаще можно встретить информацию об использовании беспилотных летательных аппаратов в целях нанесения ущерба и вреда. Например, в 2019 г. на крупных месторождениях компании Saudi Aramco в Абкайке и Хурайсе (Саудовская Аравия) произошли пожары, причиной которых стала атака беспилотных летательных аппаратов [20]. В марте 2022 г. нефтеперерабатывающий завод в Эр-Рияде (Саудовская Аравия) был также атакован беспилотниками [21]. Еще одним примером является удар беспилотника в Кабуле (Афганистан), в котором погибли 10 человек, за несколько дней до вывода из Афганистана войск США. Генерал Центрального командования США при этом отметил, что американская разведка следила за машиной сотрудника гуманитарной организации, подозревая, что он был связан с организацией «Исламское государство» (организация признана террористической в соответствии с резолюцией 1267 (1999) Совета Безопасности ООН), однако подтверждения в дальнейшем найдено не было [22].

Террористические организации используют информационное пространство в преступных целях для совершения террористических преступлений, в частности, для пропагандистской деятельности, осуществления вербовки в террористические ряды, подстрекательства к совершению террористических преступлений. В общем и целом, представляется очевидным, что информационное пространство является наиболее «удобной» территорией для преступной, в частности, террористической деятельности, поскольку отличается оперативностью, экономичностью и доступностью; слабой цензурой или полным отсутствием цензуры; наличием большой аудитории пользователей; быстрым и относительно дешевым распространением специально подобранной информации, комплексностью ее подачи и восприятия; анонимностью связи и скрытностью источника воздействия; возможностью несанкционированного подключения к компьютерным сетям управления стратегическим объектами, в том числе военными; дистанционным характером воздействия на компьютерные системы в различных регионах мира и др. [23].

Интересным примером использования информационного пространства в террористических целях является, журнал «Inspire», интернет-издание,

выпускаемое «Аль-Каидой» (организация признана террористической в соответствии с резолюцией 1267 (1999) Совета Безопасности ООН) с целью дать мусульманам возможность готовиться к участию в джихаде. В журнале содержатся идеологические материалы, направленные, как отмечается, на поощрение терроризма [24, с. 8]. На наш взгляд, понятие «кибертерроризм» довольно многогранное и может объединять в себе различные проявления терроризма в информационном пространстве. Представляется справедливым мнение УНП ООН о том, что не только конкретные акты с целью повреждения критически важное инфраструктуры являются кибертерроризмом. Использование, например, беспилотных летательных аппаратов, работающих с помощью различных программных обеспечений или создание атмосферы страха и угрозы жизни, осуществляющиеся с помощью массовых рассылок в интернете, также могут рассматриваться как подпадающие под понятие «кибертерроризм».

Нарушение прав человека. Меры, принимаемые государствами в контексте борьбы с терроризмом (кибертерроризмом), могут ставить под угрозу реализацию прав человека. Совет Безопасности ООН в своих резолюциях (1456 от 20 января 2003 г., 2178 от 18 сентября 2014 г., 2395 от 21 декабря 2017 г.) отмечает, что государства должны соблюдать права человека в рамках проведения контртеррористических операций. Специальный докладчик по вопросам поощрения и защиты прав человека и основных свобод в условиях борьбы с терроризмом указывает, в частности, на необходимость защиты права на жизнь, осуществления справедливого и беспристрастного расследования в ходе борьбы с терроризмом, защиты жертв терроризма (доклад 34/61 (2017)), соблюдение прав человека при объявлении чрезвычайной ситуации в государстве из-за террористических угроз (доклад 37/52 (2018)). Отдельным аспектом, вызывающим беспокойство, является введение без каких-либо расследований и судебных разбирательств санкций против лиц, которые, по мнению того или иного государства, причастны к преступной деятельности.

В науке международного права обсуждается аспект правомерности/неправомерности осуществления целенаправленного убийства лиц, подозреваемых в терроризме (*Targeted Killing of Suspected Terrorists*), в частности, вопрос о том, можно ли рассматривать подозреваемых в терроризме в качестве «законной военной цели» во время вооруженных конфликтов, вне зависимости от того, носит конфликт международный или немеждународный характер. Прежде всего, ст. 6 Международного пакта о гражданских и политических правах 1966 г. определяет, что «право на жизнь есть неотъемлемое право каждого человека. Это право охраняется законом. Никто не может быть произвольно лишен жизни». Одновременно с этим международное гуманитарное право (далее – МГП) защищает лиц, более не принимающих

участие в военных действиях и гражданское население, в частности, МГП защищает всех лиц от произвольного и незаконного лишения жизни, а также указывает на необходимость проведения надлежащих судебных процедур в рамках привлечения к ответственности за участие в военных действиях без права на это, за военные преступления и иные преступления [25, с. 45]. Более того, такого рода действие, как лишение жизни подозреваемых в терроризме лиц, может быть квалифицировано как применение смертной казни без соблюдения каких-либо норм, что противоречит международным стандартам осуществления правосудия за международные преступления, в том числе военные [11, с. 262].

Нехватка квалифицированных специалистов в области противодействия кибертерроризму. Обучение, проведение учений и наличие квалифицированного персонала являются важнейшими областями, определяющими успех в деятельности по борьбе с преступлениями в информационном пространстве [26, с. 60]. Вместе с тем одной из проблем в области противодействия кибертерроризму сегодня является нехватка квалифицированных специалистов в сфере кибербезопасности. Сотрудникам правоохранительных органов может не хватать навыков и опыта проводить работу по выявлению преступлений и виновных в преступлениях в сфере информационной безопасности. Безусловно, для такой работы необходимо освоение специальных программ, а также постоянное повышение квалификации, что обусловлено быстроразвивающейся сферой информационных технологий и растущей угрозой совершения новых преступлений в информационном пространстве.

Подводя итог можно отметить, что вышерассмотренные факторы оказывают негативный эффект на действенное противодействие кибертерроризму, в связи с чем представляется необходимым.

1. Разработать и закрепить понятие «кибертерроризм» в соответствующих законодательных актах.

2. Правоохранительным органам и иным специализированным учреждениям государств эффективно взаимодействовать между собой, а также с международными организациями с целью обмена опытом в деле борьбы с кибертерроризмом.

3. Пресекать акты кибертерроризма на стадии их подготовки, проводить мониторинг состояния информационно-коммуникационного пространства [27, с. 16].

4. Обеспечивать соответствие принимаемых мер по борьбе с терроризмом международному праву прав человека, международному гуманитарному праву.

5. При отсутствии вносить соответствующие изменения и дополнения, предусматривающие ответственность за совершение кибертерроризма, в национальное уголовное законодательство.

6. Создать аппарат, специализирующийся на выявлении и раскрытии преступлений в киберпространстве.

7. Осуществлять специальную подготовку кадров для работы с раскрытием преступлением в информационном пространстве.

Библиографический список

1. «Объединиться для противодействия терроризму» – комментарий Генерального секретаря о конференции Организации Объединенных Наций высокого уровня по борьбе с терроризмом 26 июня 2018 г. // Организация Объединенных Наций [Электронный ресурс]. – Режим доступа: https://www.un.org/sg/ru/content/sg/articles/2018-06-26/uniting-world-against-terrorism. – Дата доступа: 25.03.2022.

2. Резолюция Совета Безопасности Организации Объединенных Наций 2462 (2019) // Организация Объединенных Наций [Электронный ресурс]. – Режим доступа: https://undocs.org/S/RES/2462(2019). – Дата доступа: 25.03.2022.

3. Резолюция Совета Безопасности Организации Объединенных Наций 1624 (2005) // Организация Объединенных Наций [Электронный ресурс]. – Режим доступа: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/510/54/PDF/N0551054.pdf?OpenElement. – Дата доступа: 25.03.2022.

4. Резолюция Совета Безопасности Организации Объединенных Наций 2354 (2017) // Организация Объединенных Наций [Электронный ресурс]. – Режим доступа: https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=S/RES/2354(2017)&Lang=R. – Дата доступа: 25.03.2022.

5. Террористы осваивают киберпространство и вербуют «одиночек» // Организация Объединенных Наций [Электронный ресурс]. – Режим доступа: https://news.un.org/ru/story/2021/01/1394092. – Дата доступа: 25.03.2022.

6. Мазуров, В. А. Кибертерроризм: понятие, проблемы противодействия / В. А. Мазуров / Доклады ТУСУР. – 2010. – № 1(21). – Ч. 1. – С. 41–45.

7. Антонян, Е. А. Блокчейн технологии в противодействии рискам кибертерроризма / Е. А. Антонян. – Москва : Научный консультант, 2019. – 60 с.

8. Голубев, В. А. Кибертерроризм как новая форма терроризма [Электронный ресурс]. – Режим доступа: https://www.crime-research.ru/library/Gol_tem3.htm. – Дата доступа: 25.03.2022.

9. Довгань, Е. Ф. Права человека в контексте борьбы с международным терроризмом /Е. Ф. Довгань // Труд. Профсоюзы. Общество. – 2019. – №2. – С. 54–60

10. Довгань, Е. Ф. Правомерность целевых санкций Совета Безопасности ООН в рамках борьбы с терроризмом / Е. Ф. Довгань // Право.by. – 2011. – № 3. – С.11–21.

11. Douhan, A. F. Adapting the Human Rights System to the Cyber Age /A. F. Douhan // Max Planck Yearbook of United Nations Law Online. – 2020. – № 23 (1). – P. 249–289.

12. Мороз, Н. О. Международно-правовая квалификация кибертерроризма / Н.О. Мороз / Вестник Марийского государственного университета. Серия «Исторические науки», «Юридические науки». – 2016. – № 2 (6). – С. 79–82.

13. Tafoya, W. L. Cyber Terror [Electronic resource]. – Mode of access: https://leb.fbi.gov/articles/featured-articles/cyber-terror. – Date of access: 25.03.2022.

14. Голубев, В. А., Сайтарлы, Т. А. Проблемы борьбы с кибертерроризмом в современных условиях [Электронный ресурс]. – Режим доступа: https://www.crime-research.org/library/e-terrorism.htm. – Дата доступа: 25.03.2022.

15. Lewis, J. A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats [Electronic resource]. – Mode of access: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf. – Date of access: 28.03.2022.

16. Denning, D. E. Is Cyber Terror Next? [Electronic resource]. – Mode of access: http://essays.ssrc.org/sept11/essays/denning.htm. – Date of access: 28.03.2022.

17. Кибертерроризм [Электронный ресурс]. – Режим доступа: https://www.unodc.org/e4j/ru/cybercrime/module-14/key-issues/cyberterrorism.html. – Дата доступа: 25.03.2022.

18. Что такое сваттинг и какая ответственность за него предусмотрена? [Электронный ресурс]. – Режим доступа: https://centr.minsk.gov.by/be/sfery-deyatelnosti/zakonnost-i-pravoporyadok/pravookhranitelnye-organy/ruvd-tsentralnogo-rajona-g-minska/novosti-ruvd-tsentralnogo-rajona-g-minska/10672-chto-takoe-svatting-i-kakaya-otvetstvennost-za-nego-predusmotrena. – Дата доступа: 25.03.2022.

19. ФСБ раскрыла, кто стоит за ложными минированиями в России [Электронный ресурс]. – Режим доступа: https://www.gazeta.ru/social/2022/02/10/14519713.shtml. – Дата доступа: 25.03.2022.

20. Атака дронов на нефтяные объекты Саудовской Аравии. Главное [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/politics/14/09/2019/5d7d05639a79479b16755e08. – Дата доступа: 25.03.2022.

21. В Саудовской Аравии беспилотники атаковали нефтеперерабатывающий завод [Электронный ресурс]. – Режим доступа: https://eadaily.com/ru/news/2022/03/11/v-saudovskoy-aravii-bespilotniki-atakovali-neftepererabatyvayushchiy-zavod. – Дата доступа: 25.03.2022.

22. США признали, что их беспилотник по ошибке убил в Кабуле мирных афганцев [Электронный ресурс]. – Режим доступа: https://www.bbc.com/russian/news-58604726. – Дата доступа: 28.03.2022.

23. Киберпространство и информационный терроризм [Электронный ресурс]. – Режим доступа: http://scienceport.ru/news/kiberprostranstvo-i-informatsionnyy-terrorizm/. – Дата доступа: 28.03.2022.

24. Использование Интернета в террористических целях [Электронный ресурс]. – Режим доступа: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf. – Дата доступа: 28.03.2022.

25. Targeted Killing of Suspected Terrorists During Armed Conflicts: Compatibility with the Rights to Life and to a Due Process [Electronic resource]. – Mode of access: https://www.corteidh.or.cr/tablas/r27148.pdf. – Date of access: 28.03.2022.

26. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства // Организация по безопасности и сотрудничеству в Европе [Электронный ресурс]. – Режим доступа: https://www.osce.org/files/f/documents/5/2/110472.pdf. – Дата доступа: 25.03.2022.

27. Молодчая, Е. Н. Политика противодействия кибертерроризму в современной России: политологический аспект: автореф. дис. ... канд. полит. наук : 23.00.02 / Е. Н. Молодчая ; ФГБОУ ВПО «Российский государственный социальный университет». – Москва, 2011. – 30 с.