УДК 323.28+004.738.5:303.833.6 https://doi.org/10.24158/pep.2018.6.5

Симонова Эллада Юрьевна

соискатель кафедры прикладного анализа международных проблем Московского государственного института международных отношений (университета) Министерства иностранных дел Российской Федерации

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОСНОВНЫХ ПОДХОДОВ К ОПРЕДЕЛЕНИЮ КИБЕРТЕРРОРИЗМА В СОВРЕМЕННОЙ МИРОВОЙ ПОЛИТИЧЕСКОЙ НАУКЕ

Аннотация:
В статье прослеживается развитие подходов в современной мировой политической науке к определению кибертерроризма начиная с 1980-х гг., когда данный термин появился впервые. Представлены работы преимущественно американских авторов, так как сам термин и основные подходы к его определению были сформулированы в США. Объясняется основная разница в подходах представителей научных кругов и общественности к определению кибертерроризма, приводятся возможные причины существующего несоответствия между ними. Автор описывает узкое и более широкое толкования кибертерроризма, или кибертерроризм в чистом виде и традиционный кибертерроризм, и анализирует недостатки последнего. Показано главное различие между кибертерроризмом и киберпреступностью. Приводится понятие «цифрового джихада», или «терроризма в киберпространстве», сформулированное в качестве альтернативы спорам вокруг узкого и широкого определений кибертерроризма. Сделан вывод о необходимости дальнейшего изучения проблемы кибертерроризма, даже в отсутствие его общепринятого определения.

Ключевые слова:
киберпространство, терроризм, террористический акт, понятие кибертерроризма, киберпреступность, хакерские атаки, информационная безопасность, сеть Интернет.

Simonova Ellada Yuryevna

External PhD student, Department of Applied International Analysis, Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation

A COMPARATIVE ANALYSIS OF THE MAIN APPROACHES TO DEFINING CYBERTERRORISM IN MODERN WORLD POLITICAL SCIENCE

Summary:
The research described the development of the notion of cyberterrorism in global political science since the 1980s when it was first introduced. The paper presented the works of American scientists mainly because the term and the main approaches to defining it were forged in the USA. The research explained the main difference between scientific and public approaches to defining cyberterrorism and provided possible reasons for discrepancy between them. Cyberterrorism, or pure cyberterrorism and traditional cyberterrorism, was interpreted in a narrow and broad sense, and the drawbacks of the latter were analyzed. Besides, the main difference between cyberterrorism and cybercrime was demonstrated. Moreover, the author introduced the concept of digital jihad, or terrorism in cyberspace, forged as an alternative to debates on the narrow and broad definitions of cyberterrorism. It is concluded that further consideration of cyberterrorism is essential despite the absence of its universal definition.

Keywords:
cyberspace, terrorism, terrorist attack, notion of cyberterrorism, cybercrime, hacking attacks, information security, the Internet.

Начиная с XIX в. и по настоящий день в мире предпринимаются непрестанные, но безуспешные попытки сформулировать общепринятое определение терроризма. Одной из причин, затрудняющих достижение поставленной цели, является слишком большое многообразие его форм. При этом международный терроризм не прекращает трансформироваться, порождая в научной среде дебаты относительно определения его новых проявлений – в первую очередь использования террористическими организациями киберпространства.

Исследование киберугроз, и в частности кибертерроризма, с целью выработки эффективных мер противодействия им отличается большой актуальностью, учитывая быстрое развитие информационных технологий в мире и глобальный характер террористической угрозы. Общепринятое определение кибертерроризма на сегодняшний день отсутствует, причем некоторые исследователи выступают против выделения данного понятия. В статье рассмотрены основные подходы в современной политической науке к определению понятия кибертерроризма, споры вокруг которого носят еще более ожесточенный характер, нежели вокруг определения терроризма.

Термин «кибертерроризм» был введен в 1980-е гг. старшим научным сотрудником американского Института безопасности и разведки Б. Коллином для обозначения новой формы террористической деятельности [1, p. 15]. Сперва он имел номинальное значение, но получил развитие в 1990-е гг. – в ответ на возросшее тогда в мире использование сети Интернет и первые кибератаки.

Спецагент ФБР М. Поллитт предложил следующее определение кибертерроризма: «Преднамеренная, политически мотивированная атака на информацию, компьютерные системы, программы и базы данных, которая результирует в насилие против некомбатантов со стороны субнациональных группировок или подпольно действующих агентов» [2, p. 9].

Определение М. Поллитта складывается из двух компонентов: киберпространства и терроризма. Под киберпространством подразумевается «место, где функционируют компьютерные программы и перемещаются данные» [3]. В отсутствие общепринятого понятия терроризма М. Поллитт взял за основу определение, выработанное Государственным департаментом США: «Терроризм – это преднамеренное, политически мотивированное насилие в отношении некомбатантов со стороны субнациональных группировок или подпольно действующих агентов» [4].

В 2000 г. профессор Джорджтаунского университета Д. Дэннинг расширила понятие и определила кибертерроризм как «противозаконные атаки или угрозы атак на компьютеры, сети и хранимую в них информацию для устрашения или принуждения правительства или граждан к какому-либо действию в политических или общественных целях» [5]. Позднее профессор уточнила, что актами кибертерроризма могут считаться только те атаки, которые результируют в насилие против людей или собственности, либо наносят урон, достаточный для порождения страха. В качестве примеров – атаки, которые приводят к гибели людей, взрывам, авиакрушениям, заражению воды и др. [6, p. 125].

В то время как угроза киберпреступности в мире постоянно росла и развивалась, угроза кибертерроризма так и осталась теоретической. Отсутствие конкретных примеров дало начало дискуссии о том, не является ли кибертерроризм выдумкой.

В противоположность научным дискуссиям о существовании кибертерроризма термин получил широкое распространение в публичном пространстве: журналисты и политики популяризовали идею о грядущем кибертеракте, который поставит под удар жизни миллионов людей и всю систему национальной безопасности. СМИ начали усматривать возможные примеры кибертерроризма в каждой хакерской атаке на правительственные сайты.

Анализируя описываемые в прессе сценарии возможных кибертеррористических атак, эксперты по проблемам кибербезопасности указывают на их нереалистичность. Это связано с тем, что критически важные объекты (например, комплексы ядерного оружия) не подключаются к какой-либо открытой компьютерной системе, а также с тем, что на настоящий момент у террористов нет возможностей для осуществления таких атак [7].

Считая угрозу кибертерроризма незначительной, известный в мире специалист по проблемам терроризма в киберпространстве, профессор факультета коммуникаций Университета Хайфы Г. Вейманн объясняет чрезмерное внимание общественности к проблеме целым рядом причин [8]. Во-первых, это дань моде. Во-вторых, многие СМИ не способны различить кибертерроризм и хакеризм. В-третьих, многие люди до конца не понимают и поэтому боятся таких понятий, как «терроризм» и «технологии». В-четвертых, некоторые политики намеренно спекулируют на тему кибертеракт, продвигая свои политические программы. В-пятых, определенную роль сыграла неоднозначность самого понятия кибертерроризма, которое привело общественность в замешательство.

Отсутствие примеров, прямой связи с насилием и огульное применение термина в СМИ привели к тому, что ряд исследователей выступили против выделения кибертерроризма как типа террористической деятельности. Ректор Оксфордского университета и известный специалист по проблемам терроризма Л. Ричардсон назвала использование термина некорректным, поскольку к терроризму относятся действия, связанные с применением насилия либо с угрозой его применения [9, p. 25]. По мнению эксперта, дезорганизация или саботаж информационных систем требуют использования иной терминологии.

Большинство исследователей, однако, считают использование понятия кибертерроризма правомерным, хотя его угрозу находят пока маловероятной. Кибератаки террористической организации могут сразу не иметь последствий в виде жертв, но могут содержать такую вероятность, посеяв страх среди населения перед возможностью того, что террористы, например, получат доступ к управлению критически важными объектами инфраструктуры государства. Согласно теореме одного из лидеров Чикагской социологической школы У. Томаса, ситуации, определяемые людьми как реальные, реальны по своим последствиям [10].

Как подчеркивает Г. Вейманн, угроза кибертерроризма может быть преувеличенной, но ее нельзя игнорировать [11].

М. Поллитт и Д. Дэннинг объясняют, как понятие кибертерроризма выстраивается из соотношения терминов «терроризм» и «киберпространство» и теряет без них всякий смысл. Однако они концентрируются только на одном аспекте слияния терроризма и киберпространства – на атаках на компьютеры, сети и хранимую в них информацию, тогда как процесс слияния касается любого примера использования террористами возможностей виртуального мира для достижения

своих целей [12]. Известные американские специалисты по компьютерной безопасности С. Гордон и Р. Форд решили назвать описываемый Д. Дэннинг аспект «кибертерроризмом в чистом виде» и предложили выделить «традиционный кибертерроризм», при котором компьютеры могут быть не только целью, но и средством атаки [13].

Предложенный подход был поддержан рядом экспертов, которые согласились с тем, что кибертерроризм должен включать в себя «любой акт терроризма, при осуществлении которого информационные системы или компьютерные технологии выступают в качестве мишени или средства нападения» [14]. Американские исследователи Б. Нельсон, Р. Чой, М. Якобуччи, М. Митчелл и Ф. Гэннон предложили добавить в эту категорию физические атаки на информационную инфраструктуру [15, p. 9–10].

Вместе с тем названные авторы не согласились с отнесением к кибертерроризму «любого примера использования террористами возможностей виртуального мира», выделив две новые категории, к которым может быть отнесена указанная активность: «кибертеррористическая поддержка» и «использование террористами сети Интернет» [16]. Под первой категорией подразумевается незаконное использование террористами информационных систем, которое само по себе не направлено на принуждение целевой аудитории к каким-либо действиям или решениям. Кибертеррористическая поддержка призвана усилить другие террористические акты. Иными словами, использование террористами информационных технологий в качестве поддержки своих противоправных действий не может классифицироваться как кибертерроризм. Примечательно, что многие российские исследователи, включая С.М. Иванова и О.Г. Томило, также придерживаются более широкого подхода к толкованию кибертерроризма, относя к нему в том числе проведение информационно-психологических операций [17, с. 83].

Тем не менее представляется затруднительным отличить террористическую атаку, осуществленную посредством использования информационных систем, от атаки, при подготовке которой такие системы использовались, но не были прямым средством нападения.

Г. Вейманн ушел от споров вокруг чистого и традиционного типов кибертерроризма, сформулировав термин «цифровой джихад», или «терроризм в киберпространстве». По словам исследователя, террористическая организация «Исламское государство» (запрещена в России) использует киберпространство по целому ряду направлений: проведение психологической войны, поиск информации, обучение террористов, сбор и перевод денежных средств, пропаганда, вербовка, организация террористических сетей, планирование и координирование террористических действий [18, p. 3]. Подход Г. Вейманна фактически разделяет и ООН, которая в отсутствие официального определения кибертерроризма называет его вышеперечисленные проявления «использованием сети Интернет в террористических целях» [19]. Кроме того, ООН солидарна с идеей о проведении различия между кибертерроризмом и киберпреступностью. С таким подходом согласна и ШОС, хотя приводимое в Соглашении о сотрудничестве в области обеспечения международной информационной безопасности различие между информационной преступностью и информационным терроризмом довольно размыто: «информационная преступность – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях»; «информационный терроризм – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях» [20].

Многие авторы, пишущие о проблеме кибертерроризма, вовсе не приводят в своих трудах его определение [21].

Параллельно дискуссии о ранжировании разных типов террористической деятельности в сети в научном сообществе ведутся споры о дифференцировании кибертерроризма и киберпреступности.

Предложенные М. Поллиттом и Д. Дэннинг определения, наиболее цитируемые в политической науке, содержат указание на насилие как обязательную характеристику кибертерроризма, которая отличает его от обычных киберпреступлений, и в частности хактивизма – деятельности в киберпространстве, направленной на выявление и использование уязвимостей в компьютерных операционных системах в политических целях [22].

Профессор Городского университета Дублина М. Конвей предложила добавить кибертерроризм в классификацию, разработанную старшим вице-президентом по вопросам информационной безопасности компании Control Risks Group К. Андерсоном для категорирования неправомерных действий в сети Интернет, которые подразделяются на «использование», «злоупотребление» и «использование в целях нападения» [23, p. 90–91]. Под вторую категорию попадает большинство хакерских атак на вычислительные системы, под третью – те атаки, которые привели к краже данных или другому ощутимому ущербу. Под кибертерроризмом понимаются «атаки, которые результируют в насилие против людей или собственности, либо наносят урон, достаточный для порождения страха» (определение Д. Дэннинг). Новая классификация, однако, не получила широкого использования ни в научных кругах, ни среди юристов, ни в СМИ.

Террористическая угроза становится более изощренной и распространенной. Не связанные инертностью развития государственных институтов террористические организации гораздо быстрее берут на вооружение перспективные информационные технологии для организации терактов и распространения своей идеологии [24].

Сегодня борьба с терроризмом и террористическая деятельность неразрывно связаны с использованием киберпространства. Ввиду фактического военного поражения террористической группировки «Исламское государство» противодействие терроризму в киберпространстве приобретет еще большую актуальность.

Учитывая постоянно нарастающее значение и быстрое развитие информационных технологий, нельзя также исключать, что террористическая киберугроза может из потенциальной превратиться в реальную. В связи с этим угроза кибертерроризма требует пристального наблюдения и изучения.

Наличие общепринятого определения кибертерроризма, возможно, не является залогом выработки эффективных мер противодействия данному явлению. С точки зрения сил безопасности борьба с кибертерроризмом не стоит особняком, поскольку осуществляется так же, как борьба с киберпреступностью и терроризмом в целом. Выявление различий между кибертеррористическими и хакерскими атаками на практике имеет значение лишь после их совершения – на этапе судопроизводства, при выборе меры наказания.

Несмотря на отсутствие единого мнения по вопросу определения кибертерроризма, необходимо продолжать следить за использованием террористами возможностей виртуального мира для профилактики, предотвращения или своевременного реагирования на угрозу чистого или традиционного кибертерроризма.

Ссылки:

1. Collin B.C. The Future of Cyber Terrorism // Crime & Justice International. 1997. Vol. 13, no. 2. March. P. 15–18.
2. Pollitt M. Cyberterrorism: Fact or Fancy? // Computer Fraud and Security. 1998. No. 2. P. 8–10. https://doi.org/10.1016/S1361-3723(00)87009-8.
3. Ibid.
4. 1996 Patterns of Global Terrorism Report [Электронный ресурс] // U.S. Department of State Archive. URL: https://1997-2001.state.gov/global/terrorism/1996Report/1996index.html (дата обращения: 24.06.2018).
5. Denning D.E. Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives [Электронный ресурс]. 2000. May 23. P. 1. URL: http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf (дата обращения: 24.06.2018).
6. Denning D.E. A View of Cyberterrorism Five Years Later // Internet Security: Hacking, Counterhacking, and Society / ed. by K. Himma. Sudbury, MA, 2006. P. 123–141.
7. Green J. The Myth of Cyberterrorism [Электронный ресурс] // Washington Monthly. 2001. Nov. 1. URL: https://washingtonmonthly.com/2001/11/01/the-myth-of-cyberterrorism/ (дата обращения: 24.06.2018).
8. Weimann G. Cyberterrorism: How Real Is the Threat? [Электронный ресурс] : special report 119 / United States Institute of Peace. Washington, DC, 2004. URL: https://www.usip.org/sites/default/files/sr119.pdf (дата обращения: 24.06.2018).
9. Richardson L. What Terrorists Want: Understanding the Enemy, Containing the Threat. N. Y., 2006. 336 p.
10. Thomas W., Znaniecki F. The Polish Peasant in Europe and America [Электронный ресурс]. Vol. V. Chicago, 1920. URL: https://archive.org/stream/polishpeasantine05thomuoft/polishpeasantine05thomuoft_djvu.txt (дата обращения: 24.06.2018).
11. Weimann G. Op. cit.
12. Gordon S., Ford R. Cyberterrorism? Symantec Security Response [Электронный ресурс] : white paper. 2003. URL: https://www.symantec.com/avcenter/reference/cyberterrorism.pdf (дата обращения: 24.06.2018).
13. Ibid.
14. Mates M. Technology and Terrorism. Brussels, 2001.
15. Cyberterror Prospects and Implications / B. Nelson, R. Choi, M. Iacobucci, M. Mitchell, F. Gagnon / Centre for the Study of Terrorism and Irregular Warfare. Monterey, CA, 1999. 145 p.
16. Ibid.
17. Иванов С.М., Томило О.Г. Международно-правовое регулирование борьбы с терроризмом // Право и безопасность. 2013. № 3–4 (45). С. 82–87.
18. Weimann G. Terrorism in Cyberspace: The Next Generation. N. Y., 2015. 344 p.
19. The Use of the Internet for Terrorist Purposes [Электронный ресурс] / United Nations Office on Drugs and Crimes in collaboration with the United Nations Counter-Terrorism Implementation Task Force. N. Y., 2012. URL: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (дата обращения: 24.06.2018).
20. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] : вступило в силу для РФ 2 июня 2011 г. // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/902289626 (дата обращения: 24.06.2018).
21. Brenner S.W., Goodman M.D. In Defense of Cyberterrorism: An Argument for Anticipating Cyber-attacks // University of Illinois Journal of Law, Technology and Policy. 2002. No. 1. P. 1–57 ; Dunnigan J.F. The Next War Zone: Confronting the Global Threat of Cyberterrorism. N. Y., 2003. 320 p.
22. Weimann G. Cyberterrorism: The Sum of All Fears? // Studies in Conflict & Terrorism. 2005. Vol. 28, no. 2. P. 129–149.
23. Conway M. Cyberterrorism: Hype and Reality // Information Warfare: Separating Hype from Reality / ed. by E.L. Armistead. Washington, DC, 2007. P. 73–94.
24. Федоров А.В. Информационная безопасность в мировом политическом процессе. М., 2006. 220 с.