УДК 32

Кибертерроризм как актуальная проблема современного мирового порядка

Пинчук Андрей Юрьевич

Кандидат политических наук,
Первый проректор,
Московский государственный технологический университет «СТАНКИН»,
127994, Российская Федерация, Москва, Вадковский переулок, 1;
e-mail: a.pinchuk@stankin.ru

Аннотация

В настоящей статье автором рассмотрены основные особенности такого явления современного мира как кибертерроризм. Отмечено, что кибератаки становятся все более привлекательным способом для террористов в связи с тем, что для их реализации требуется меньшее количество людей и значительно меньшие средства. Сделан вывод, что кибертерроризм можно считать преднамеренным использованием подрывной деятельности или угрозы таковой в отношении компьютеров и/или сетей с намерением причинить вред или достигнуть иных социальных, идеологических, религиозных, политических или аналогичных целей с запугиванием определенных граждан или иных лиц в интересах достижения подобных целей. Кибертерроризм можно считать преднамеренным использованием подрывной деятельности или угрозы таковой в отношении компьютеров и/или сетей с намерением причинить вред или достигнуть иных социальных, идеологических, религиозных, политических или аналогичных целей с запугиванием определенных граждан или иных лиц в интересах достижения подобных целей. При этом все же необходимо осознавать, что кибертерроризм это совсем не единственный фактор, угрожающий инфраструктуре современной цивилизации, но он может становиться существенным элементов комплексных деструктивных процессов.

Для цитирования в научных исследованиях

Пинчук А.Ю. Кибертерроризм как актуальная проблема современного мирового порядка // Теории и проблемы политических исследований. 2018. Том 7. № 5А. С. 88-95.

Ключевые слова

Кибертерроризм, киберсреда, кибератака, терроризм, террористический акт, противодействие кибертерроризму, кибербезопасность.

Введение

Понятие «кибертерроризм» приобрело свою ясность в конце XX века. По своей сути оно означает использование киберпространства и его инструментов в террористических целях, в основном в политических или идеологических целях. Кибертерроризм сам по себе является наиболее важным фактором в деле изменения облика современного терроризма. Это происходит в точке пересечения двух разных миров – физического и виртуального. И что важно, все находится в конвергенции этих двух измерений. В век увеличения онлайн-атак и террористической активности, страх перед кибертерроризмом имеет возрастающую тенденцию. Данный термин был введен в 1980-х Барри Коллином, который указал, что как физический, так и виртуальный мир начали сливаться и трансформироваться в некоторую особую форму терроризма. Термин распространился быстро и с этого момента стал использоваться правоохранительными органами, учеными и средствами массовой информации. Серьезную опасность кибертерроризма во многом обусловлена не восприятием национальных границ при осуществлении таких террористических акций, которые могут быть осуществлены из любой точки мира. При этом террористы могут действовать как против гражданских, так и против военных объектов.

В этой связи необходимо выделить критерии кибертерроризма. Это, во-первых среда и технологии, он должен осуществляться через киберпространство; во-вторых, он должен быть неизбежно политическим или идеологическим по целям и мотивам; в-третьих, он должен быть насильственным или угрожать насилием; в-четвертых, он должен иметь далеко идущие психологические последствия, выходящие за рамки непосредственной жертвы или цели; в-пятых, он должен проводиться либо силами организации с конкретным задачами или конспиративными ячейками или отдельными представителями террористического движения; и, наконец, он должен быть совершен субнациональными группами или негосударственными образованиями.

Основная часть

Основная сфера применения кибертерроризма включает большие промышленные системы, такие как электростанции, водяные плотины или заводы, где почти все контролируется кибернетическими технологиями, которые выступают как наиболее эффективный и действенный инструмент [Brennan, 2012, 2-3]. Эти большие системы не только там, где виртуальный мир управления встречается с физической реальностью, но и там, где может возникнуть единая «точка отказа» и, таким образом, повлиять на повседневную жизнь тысяч людей. Необходимо признать, что кибернетические технологии в значительной степени оказали влияние на организацию и деятельность террористических групп. Данные технологии позволили ускорить переход от иерархической к децентрализованной сетевой структуре, что обеспечило повышение эффективности террористической деятельности.

К основным задачам терроризма в киберпространстве следует отнести попытки воспрепятствования или разрушение процесса функционирования компьютерных систем или сетей информационной инфраструктуры государства или органов управления. Подобные преступные действия в отношении критически важных объектов информационной инфраструктуры представляют собой значительную угрозу, которая может иметь самые серьезные последствия для всего общества.

В этой связи необходимо определить, почему использование киберпространства так привлекательно для террористов и какие способы и методы атак они могут применить. Прежде всего, для большей ясности в вопросе об угрозах национальной безопасности государств, исходящих из киберпространства, формах и способах противоборства в нем необходимо сформулировать определение собственно киберпространства (cyberspace). Террористическое киберпространство включает в себя использование информационно-коммуникационных технологий, которые разработаны или предназначены для уничтожения или серьезного нарушения ключевых объектов инфраструктуры или важной информации [Schjolberg, 2011, 49].

Категорией киберпреступности и криминального злоупотребления возможностями информационно-коммуникационных технологий в киберпространстве являются террористические атаки. Для описания этого явления часто используется термин «кибертерроризм», но при его использовании важно понимать, что это не совсем новая категория преступлений. Кибертерроризм предназначен для запугивания или принуждения правительства, народа к определенным политическим или социальным действиям. Согласно этой логике, атака должна приводить к насилию в отношении лиц или имущества, или, по меньшей мере, наносить серьезный ущерб.

Следует указать и на то, что основная цель кибертеррориста не обязательно состоит в уничтожении, дезинтеграции или дезинформации объектов в киберпространстве. Приоритетной задачей может быть использование Всемирной сети для «усиления» воздействий некоторых других физических угроз или актов терроризма. Эта деятельность включает, например, мероприятия по сбору разведывательной информации, поддержанию связи, координации материально-технического обеспечения и управлению общественным мнением, т.е. подаче информации, выгодной с точки зрения террористов. При этом уровень технических возможностей может в итоге стать решающим фактором при выборе террористической организацией киберпространства как оперативной сферы своей деятельности [Gordon, 2003, 8].

Исходя из этого, следует констатировать развитие тенденций к росту технологической подготовленности террористических групп, активной интеграции кибернетических технологий в инфраструктуру террористов, а также активное применение кибертехнологий как в целях защиты, так и террористического нападения. Также следует учитывать, что не во всех случаях использование киберпространства остается полностью анонимным, ведь активное наращивание сил государственных контртеррористических структур, повышение уровня их технического оснащения, совершенствование оперативных методов деятельности может привести к отслеживанию инициаторов кибератаки.

Учитывая эти факторы, кибертеррористы должны оценить, является ли вероятность раскрытия их оперативной базы менее ценной потерей, чем результат их кибероперации. И, наконец, киберпространство относится к непредсказуемой сфере и достижение целей кибератаки не всегда гарантировано, поэтому террористы могут просто не пойти на выделение ресурсов на применение непроверенного метода. Тем не менее, отталкиваясь от методологии проведения атак, все-таки следует отнести кибертерроризм к операциям с не самыми высокими затратами. Если коротко, то большинство побудительных мотивов к проведению кибертеррористических атак весьма сходны, если вообще не одинаковы, а это переводит кибероперации в разряд очень привлекательных форм информационного противоборства. Исходя из этого, кибератаки становятся все более привлекательным способом для террористов в связи с тем, что для их реализации требуется меньшее количество людей и значительно меньшие средства [Thomas, 2005]. Если нападение считается организованной кучкой хакеров,

политически или финансово мотивированный, тогда оно может быть оценено атакуемым государством для того, чтобы определить соответствующее ответ в пределах своей компетенции. Однако транснациональный характер большинства преступных организаций в киберпространстве могут осложняться вопросом о подсудности.

Определенным шагом вперед в этой сфере стала Конвенция Совета Европы о киберпреступности, которая явилась первым международным договором, предпринявшим попытку гармонизировать законы разных стран относительно того, что представляет собой преступная деятельность в киберпространстве. Этот договор о правоприменении, также известный как Будапештская Конвенция, требует, чтобы подписавшие его стороны приняли уголовное законодательство против определенных видов деятельности в киберпространстве для расширения возможностей правоохранительных органов по расследованию такой деятельности и сотрудничеству с другими подписавшими сторонами. Хотя данная Конвенция представляется в качестве наиболее существенного международного соглашения, касающегося кибербезопасности, некоторые наблюдатели считают ее неудачной. Критики предупреждают, что Конвенция ограничена с точки зрения правоприменения и юрисдикция в странах, где преступники действуют свободно. Также следует указать и о существовании ряда резолюций Генеральной Ассамблеи ООН, касающихся кибербезопасности, принятых за последние 15 лет.

Методы кибертерроризма становятся яснее, когда человечество станет понимать общие аспекты поведения кибертеррористов. Существует три основных направления для того, чтобы физические системы могли управляться чем-то виртуальным. Первый это доступ, создание универсального интерфейса с высоким уровнем доступа к данным и информации. Второй – управление, предоставляющее (и не только) администраторам инструменты для удаленного управления системами. И последнее, но не менее важное, это интеллектуальный анализ данных, что означает получение знаний из сети. Исходя из этого, кибертеррористы обычно ищут потенциал уязвимостей для использования разрушительных действий в критической инфраструктуре.

Террористы используют киберпространство, чтобы вызвать неопределенность и смуту. Они для борьбы с государственными органами используют все имеющиеся у них средства для достижения поставленных целей. В частности, кибертеррористы в 1998 г. атаковали сайт индийской компании «Bhabha Atomic Research Center» и украли электронную переписку. Три анонимных террориста через интернет-интервью заявили, что тем самым протестуют против недавних ядерных взрывов в Индии. 9 июля 1997 года лидер китайской хакерской группы заявил, что временно блокировали китайский спутник и объявили, что хакеры создали новую глобальную организацию, протестующую и стремящуюся предотвратить инвестиции западных стран в Китай.

В сентябре 1998 года, накануне парламентских выборов в Швеции, произошло нападение кибердиверсантов на вебсайт правой политической партии Швеции и создана ссылка на вебсайт с порнографическим содержанием. В том же месяце, диверсанты атаковали сайт правительства Мексики в знак протеста против коррупции и цензуры. В августе 2012 г. серия кибератак была направлена против Saudi Aramco, крупнейшей в мире нефтегазовой компании - производителя. Атаки затронули 30 000 компьютеров, и код, по-видимому, был разработан для нарушения или остановки добычи нефти. В свою очередь кибератаки на компанию «Sony Entertainment» иллюстрируют трудности в классификации атак и разработке политики реагирования. 24 ноября 2014 г. Sony пережила кибератаку, в ходе которой были отключены информационно-технологические системы, уничтожены данные и рабочие станции, вскрыта внутренняя

электронная переписка и похищены другие материалы.

По своей сути кибертерроризм существует только в киберпространстве, следовательно, его непосредственные эффекты ограничиваются данной средой. Тем не менее, это не означает, что кибертерроризм не в состоянии воздействовать на физический, материальный мир. Следует отметить, что наступательные операции в киберпространстве с применением кибероружия, а следовательно, и кибертерроризм могут привести к кинетическим эффектам. При этом считается, что наиболее эффективным использование кибертерроризма – это когда он используется в сочетании с физическим терроризмом

Преступники и террористы в значительной степени полагаются на кибер-технологии для поддержки организационного целеполагания. Например, транснациональные террористические организации, повстанцы и джихадисты использовали Интернет как инструмент планирования атак, радикализации и вербовки, как метод пропаганды распространение своей идеологии, средство связи и в разрушительных целях.

Мотивация потенциального кибертеррориста считается очень важным аспектом, который в целом определяет уровень опасности, которую он способен генерировать. Можно выделить, в основном, два типа целей, которых хочет достичь кибертеррорист. Он либо преследует конкретную цель, например пропаганду политической идеологии или зарабатывание денег, либо преследует цель получения удовольствия и энтузиазма, вызванных потенциальным успехом. Второй случай считается очень опасным, так как будущие действия трудно предсказать, и, таким образом, очень трудно будет выполнить поиск наиболее слабого звена цепи и уязвимых мест в системе кибербезопасности.

Одним из важных факторов также является внутренний мир хакера, который обычно чувствует себя невиновным в подобного рода действиях, которые он выполняет, считая, что он делает праведную вещь. Многие террористические организации используют Интернет для массового «охвата» своей аудитории без необходимости использовать другие средства массовой информации, такие как радио, телевидение или проведение различных пресс-конференций. Их вебстраницы не отображают информацию, связанную с насильственной деятельностью, но, как правило, утверждают, что не осталось другого выбора, кроме как прибегнуть к насилию. Выраженное в таком виде публичное выступление является очень простым способом привлечь сторонников и членов в свои организации.

В этой связи кибербезопасность имеет большое значение для многих организаций, в том числе и направленная против террористов. Причина этого в первую очередь заключается в их вредоносной деятельности, поэтому очевидно, что террористы столкнутся с хорошо оснащенными правительственными силами безопасности, что позволяет этим силам легко раскрыть свои намерения посредством перехвата сообщений с помощью сложного оборудования для мониторинга. Эта проблема хорошо известна террористическим организациям и является причиной их повышенного внимания к аспектам безопасности при передаче скрытой информации. Наличие в «Аль-Каиде» учебного пособия, посвященного этому вопросу, является лишь одним из многих доказательств приверженности террористических организаций обеспечению безопасности внутренних коммуникаций. Кроме пропаганды на вебсайтах террористических организаций часто можно найти материалы и инструкции о том, как сделать взрывчатые вещества и химическое оружие. Это позволяет им идентифицировать наиболее приближенных к их идеям пользователей, позволяя развить симпатию к их делу, что является достаточно эффективным методом вербовки.

Следовательно, в настоящее время, когда речь идет об угрозе кибертерроризма, наиболее

точным было бы назвать его злонамеренным использованием интернета террористами. Так, Управление ООН по наркотикам и преступности делит кибертерроризм на шесть основных областей, а именно пропаганда, финансирование, подготовка, планирование, осуществление и кибератаки:

a. Пропаганда: онлайн-платформы резко увеличили свой потенциал для публичных заявлений террористических групп, распространения ими своих идей любыми виртуальными средствами (видео, аудио сообщения, чаты, социальные сети и т. д.). Под этим понимается также деятельность по подстрекательству, вербовке и радикализации новых филиалов.

б. Финансирование: поиск финансовых ресурсов осуществляться через несколько каналов. К ним относятся прямой подход, электронная коммерция, онлайновые платежные системы и использование очевидно, законных организаций. Возможность иметь сайты, посвященные этой деятельности, помогает террористам более эффективно осуществлять денежные транзакции.

c. Подготовка: со временем террористические группы разработали несколько способов подготовки новобранцев через интернет. Это включает в себя обмен материалами о том, как производить оружие и способы проведения атаки. Онлайн-платформы, посвященные тренировкам, могут форсировать достижение необходимого уровня новобранцами.

d. Планирование: интернет-ресурсы также облегчили планирование атаки. Сбор разведданных по заданной цели сегодня проще благодаря огромному количеству открытой исходной информации, которая доступна, от социальных сетей до географических информационных программ.

e. Выполнение: все вышеперечисленное может способствовать окончательному выполнению атаки, с дополнительным преимуществом в том, что стороны, участвующие в подготовке акта, но их достаточно сложно задержать, если они использовали правильные меры предосторожности при обмене информацией или проведении фоновых исследований.

f. Кибератаки: они также упоминаются УНП ООН, хотя они рассматриваются как тема для будущих исследований, а не для непосредственного обсуждения. Этот раздел направлен на определение кибертерроризма.

Тем не менее, было бы неразумно исключать развитие новых методик, в том числе не только компьютерных, от талибов, так как они, возможно, захотят активизировать свою деятельность, чтобы не потерять почву для ИГ (запрещенная в РФ организация). Действительно, не секрет, что ИГ (запрещенная в РФ организация) также стремится развивать свою деятельность в киберпространстве. Они называют себя «кибер-халифат» через сообщения и видео-СМИ, связанных с группировкой. Более того, им удалось осуществить серию кибератак, исключительно компьютерных, которые в одном случае даже привели к раскрытие частной информации о государственных служащих США. Такое сильное присутствие в различных слоях киберпространства также помогла привлечь внимание хакеров-единомышленников. Для выполнения атаки злоумышленник не должен фактически присутствовать на месте причиненного ущерба, и не должен иметь слишком много человеческих ресурсов. Поэтому реальная опасность заключается в превращении терроризма в кибертерроризм.

Заключение

Терроризм был привилегией больших политических движений с большими финансовыми донорами, в то время как кибертеррорист может быть единственным человеком, сидящим в комфортных условиях своего дома. Таким образом, кибертерроризм можно считать преднамеренным использованием подрывной деятельности или угрозы таковой в отношении

компьютеров и/или сетей с намерением причинить вред или достигнуть иных социальных, идеологических, религиозных, политических или аналогичных целей с запугиванием определенных граждан или иных лиц в интересах достижения подобных целей. При этом все же необходимо осознавать, что кибертерроризм это совсем не единственный фактор, угрожающий инфраструктуре современной цивилизации, но он может становиться существенным элементом комплексных деструктивных процессов.

Библиография

1. Конвенция о компьютерных преступлениях (Будапешт, 23 ноября 2001 года).
2. Brennan J.W. United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling? U.S. Army War College, 2012.
3. Gordon S. Cyberterrorism? Symantic Security Response. White Paper, 2003.
4. Schjolberg S., Ghernaouti-Helie S. A Global Treaty on Cybersecurity and Cybercrime. 2011.
5. Thomas T.L. Cyber Silhouettes: Shadows over Information Operations. Foreign Military Studies Office, Fort Leavenworth, KS, 2005.

Cyberterrorism as an actual problem of modern world order

Andrei Yu. Pinchuk

PhD in Political Science, First Pro-Rector,
Moscow State University of Technology “STANKIN”,
127994, 1, Vadkovskii lane, Moscow, Russian Federation;
e-mail: a.pinchuk@stankin.ru

Abstract

Cyberterrorism itself is the most important factor in changing the face of modern terrorism. This happens at the intersection of two different worlds, the physical and the virtual. In this article, the author discusses the main features of such a phenomenon of the modern world as cyberterrorism. It was noted that cyber-attacks are becoming an increasingly attractive way for terrorists due to the fact that they require fewer people and significantly less money. It is concluded that cyber-terrorism can be considered deliberate use of subversive activities or threats against computers and / or networks with the intent to cause harm or achieve other social, ideological, religious, political or similar goals with intimidation of certain citizens or other persons in order to achieve such goals. Cyberterrorism can be considered the deliberate use of subversion or the threat of such against computers and / or networks with the intent to cause harm or achieve other social, ideological, religious, political or similar goals with intimidation of certain citizens or other persons in order to achieve such goals. At the same time, it is still necessary to realize that cyber-terrorism is not the only factor threatening the infrastructure of modern civilization, but it can become essential elements of complex destructive processes.

For citation

Pinchuk A.Yu. (2018) Kiberterrorizm kak aktual'naya problema sovremennogo mirovogo poryadka [Cyberterrorism as an actual problem of modern world order]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 7 (5A), pp. 88-95.

Keywords

Cyberterrorism, cybercrime, cyber-attack, terrorism, terrorist act, counter-cyberterrorism, cybersecurity.

References

1. Brennan J.W. (2012) United States Counter Terrorism Cyber Law & Enabling or Disabling? U.S. Army War College.
2. (2001) Convention on computer crimes. Budapest.
3. Gordon S. (2003) Cyberterrorism? Symantic Security Response. White Paper.
4. Schjolberg S., Ghernaouti-Helie S. (2011) A Global Treaty on Cybersecurity and Cybercrime.
5. Thomas T.L. (2005) Cyber Silhouettes: Shadows over Information Operations. Foreign Military Studies Office, Fort Leavenworth, KS.