МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ

С.А. Паршин*

СОВРЕМЕННЫЕ АМЕРИКАНСКИЕ ПОДХОДЫ К ПРОБЛЕМЕ КИБЕРТЕРРОРИЗМА

Теракты 11 сентября 2001 г., продемонстрировавшие уязвимость самой мощной в военном отношении державы современного мира перед лицом нападения со стороны транснациональной сетевой террористической организации, привели к масштабным изменениям в системе обеспечения национальной безопасности в США и многих других странах. Среди угроз, противодействию которым американские правительственные структуры и эксперты сегодня уделяют повышенное внимание, особое место занимает кибертерроризм. В статье обозначены различия между понятиями «кибертерроризм», «кибервойна» и «киберпреступность»; рассмотрены ключевые характеристики кибертерроризма как специфической формы «ведения военных действий другими способами»; исследованы побудительные мотивы террористов в использовании киберпространства как оперативного поля деятельности, а также потенциальные способы организации кибератак. Особое внимание уделено анализу задач, стоящих перед США в области кибероборонны, и различных типов оборонительных и наступательных операций в киберпространстве.

Ключевые слова: США, национальная безопасность, терроризм, кибертерроризм, киберпреступность, кибервойна, некинетическая атака.

11 сентября 2011 г. исполнилось 10 лет с момента одной из самых страшных катастроф в новейшей истории США — террористических атак на здания Всемирного торгового центра в Нью-Йорке и Пентагона в Вашингтоне. Этот день без преувеличения можно назвать переломным моментом не только в истории страны, но и в отношении американцев к обеспечению безопасности своей территории, тем более что государство вследствие своей информационно-коммуникационной открытости прямо ощутило на себе полномасштабное национальное унижение, когда вопреки интересам общества его средства массовой информации на протяжении довольно длительного времени фактически работали на террористов, оказывая дестабилизирующее влияние на социальную ситуацию и уровень доверия к институтам власти.

* *Паршин Сергей Алексеевич* — полковник, научный сотрудник Центрального института военно-технической информации (e-mail: psa.vip1@mail.ru).

Именно в тот момент в силу информационной уязвимости американской формы демократии, четко осознаваемой террористами, была поставлена под сомнение способность военно-политической, экономической и финансовой мощи государства защитить жизни своих граждан и систему ценностей страны в целом.

Огромные человеческие жертвы, крупный политический, морально-нравственный и экономический ущерб, по разным экспертным оценкам превысивший 500 млрд. долл., обусловили стандартную реакцию США — поиск целей для нанесения военных ударов в рамках провозглашенной президентом Дж. Бушем-мл. сразу после терактов глобальной войны с международным терроризмом.

События 11 сентября 2001 г. послужили предлогом для начала военных операций в Афганистане и Ираке, где движение «Талибан» и диктаторский режим Саддама Хусейна были выставлены в глазах международного сообщества как главные пособники организации «Аль-Каида», взявшей на себя ответственность за теракты в США, а также для проведения широкой серии операций сил специального назначения в Ближневосточном регионе, прежде всего на Аравийском полуострове и в так называемой зоне племен в Пакистане[1], где были сосредоточены основные базы и лагеря подготовки террористов.

Однако даже с учетом очевидного успеха спецслужб США последнего времени, в том числе ликвидации в мае 2011 г. лидера «Аль-Каиды» Усамы бен Ладена, террористическая активность во всем мире остается на таком уровне, когда практически не проходит и дня, не отмеченного актами террористической направленности, получающими широкий отклик на первых полосах мировых средств массовой информации. Основной способ осуществления этих атак, как правило, состоит в применении взрывных устройств с дистанционным управлением или использовании террористов-смертников с задачей оборвать как можно больше человеческих жизней.

Вследствие этого напрашивается вполне очевидный вопрос, заботящий не только соответствующие антитеррористические и правоохранительные структуры, но и многих членов экспертного сообщества США и ведущих западных стран: «А насколько сложно в действительности спланировать и осуществить подобные атаки?». Например, еще в 2006 г. известный американский специалист в об-

[1] По классификации Министерства внутренней безопасности (МВБ) и разведывательного сообщества США, структуры «Аль-Каиды» на Аравийском полуострове обозначаются как ячейки AQAP (al-Qaida in the Arabian Peninsula), а структуры движения «Талибан» в зоне племен Пакистана — как ячейки TTP (Tehrik-e Taliban Pakistan).

ласти криптологии и компьютерной безопасности Брюс Шнайер[2] сформулировал и выложил в Интернете необычное обращение. Он предложил самой широкой аудитории пользователей Всемирной сети смоделировать и описать сценарии террористических атак в отношении ключевых компонентов критической инфраструктуры США. После анализа представленных на рассмотрение самых разнообразных сценариев Б. Шнайер, обсудив эту тему с рядом ведущих членов американского экспертного сообщества, пришел к выводу, что это далеко не такая простая задача, как кажется многим. После крупнейших в истории человечества терактов 11 сентября 2001 г. непосредственно на территории Соединенных Штатов не было осуществлено ни одной сколько-нибудь серьезной террористической атаки[3], и это с учетом того обстоятельства, что по всему миру активно действует огромное количество экстремистских группировок самого различного толка, для которых проведение атак в отношении США является приоритетной целью.

Провалы попыток экстремистов спланировать и осуществить действия, схожие по своим последствиям с терактами 11 сентября 2001 г., можно связать, безусловно, с настойчивой реализацией Вашингтоном ряда программ по глубокой модернизации всей национальной системы обеспечения безопасности, начатых после упомянутого печального события, и в первую очередь — с созданием в марте 2003 г. Министерства внутренней безопасности (МВБ), ставшего самым крупным государственным ведомством Соединенных Штатов.

За семь лет напряженной работы МВБ в кооперации с разведывательным сообществом и правоохранительными ведомствами создало и продолжает совершенствовать свою организационную

---

[2] Брюс Шнайер (Bruce Schneier) — американский криптограф, писатель и специалист по компьютерной безопасности. Президент и основатель криптографической компании «Counterpane Systems», член совета директоров Международной ассоциации криптологических исследований и член консультативного совета Информационного центра электронной приватности.

[3] По сведениям, опубликованным МВБ, наиболее активные ячейки в составе «Аль-Каиды» (ячейки AQAP) за последние годы дважды пытались совершить террористические акты, направленные против США. Так, 25 декабря 2009 г. провалилась попытка подрыва пассажирского авиалайнера, направлявшегося в район аэропорта г. Детройт, а в октябре 2010 г. была пресечена отправка в США на борту транспортного самолета начиненных взрывчатым веществом грузовых контейнеров с часовым механизмом подрыва. По оценке МВБ, ячейки «Аль-Каиды» продолжают попытки разработать инновационные методы атак, способные преодолеть систему обеспечения безопасности западных стран. Ячейки движения «Талибан» (ячейки TTP) продолжают попытки организации терактов на территории США. 1 мая 2010 г. была предотвращена попытка подрыва начиненного взрывчатым веществом автомобиля в наиболее многолюдном районе Нью-Йорка (Таймс-сквер на Манхэттене). Кроме того, движение продолжает угрожать террористическими актами, публично поклявшись отомстить за смерть Усамы бен Ладена [23].

структуру, а также формы и способы оперативной деятельности, направленные на повышение уровня защищенности национальной территории, в том числе на противодействие терроризму. В частности, МВБ выделило 18 секторов экономики в качестве элементов национальной критической инфраструктуры и ключевых ресурсов [9]. Их диапазон достаточно широк — от транспортных систем до индустриальной базы военно-промышленного комплекса. К этим элементам относятся также энергетические и финансовые системы, водные ресурсы, сельскохозяйственный комплекс и информационно-телекоммуникационные системы. Для всей критической инфраструктуры разработаны и продолжают уточняться основные руководящие документы[4] по организации и совершенствованию системы их защиты не только федеральными и местными органами власти, но и собственниками и эксплуатирующими структурами.

Стоит также отметить, что в результате активной деятельности МВБ и ФБР (Федерального бюро расследований), как подчеркивается в объединенном информационно-аналитическом бюллетене JIB (Joint Intelligence Bulletin) от 10 августа 2011 г., вероятность проведения террористических актов на территории США, посвященных годовщине печальных событий 11 сентября 2001 г., невысока: «Мы не вскрыли ни одной сколько-нибудь серьезной угрозы со стороны ячеек “Аль-Каиды” и ее союзников в желании нанести ущерб США или их интересам по всему миру и приуроченных к десятилетию террористического акта 9/11/2011, однако такие намерения у них сохраняются. Несмотря на это, мы считаем, что ячейки “Аль-Каиды” AQAP и структуры движения “Талибан” TTP, а также их союзники продолжают демонстрировать намерения и возможности по организации атак на Соединенные Штаты, хотя они не обязательно будут связаны с годовщиной террористического акта 9/11»[5] [23].

Изложенные соображения в основном касаются традиционного образа действий экстремистских группировок, когда в сознании практически любого человека слово «террорист» вызывает ассоциацию с бородатым мужчиной в чалме и Кораном в руках, приводящем в действие взрывное устройство. Однако с учетом возникновения новой сферы противоборства — киберпространства напрашивается уже другой вопрос: «А можно ли нанести ущерб, сравнимый с человеческими, политическими, экономическими и морально-нрав-

[4] Примеры руководящих документов: [18—20].

[5] Объединенный информационно-аналитический бюллетень выпускается совместно МВБ и ФБР по мере обнаружения изменений в области террористических угроз. Предназначен для своевременного предупреждения федеральных, региональных и местных органов, ответственных за реагирование на эти изменения. Выпускается по мере необходимости с 2004 г. наряду с задействованием системы экстренного оповещения о террористической опасности.

ственными потерями в результате терактов 11 сентября 2001 г., используя информационные технологии?». Как отмечают эксперты, несмотря на беспрецедентные меры по обеспечению безопасности национального киберпространства, выразившиеся, помимо множества других мер[6], в завершении формирования Министерством внутренней безопасности США в октябре 2009 г. Национального центра интеграции кибербезопасности и коммуникаций (NCCIC — National Cybersecurity and Communications Integration Center)[7], количество атак на информационно-коммуникационные ресурсы различной ведомственной принадлежности, в том числе коммерческие, продолжает увеличиваться, притом далеко не самое малое их число, по признанию самих США и ряда других развитых стран, можно рассматривать как успешные.

Следует к тому же учитывать, что террористы (помимо «Аль-Каиды» и движения «Талибан») могут осуществлять свою деятельность в самых различных формах и преследовать разные, зачастую несовпадающие цели, например политические, антигосударственные, антиглобалистские, националистические, религиозные, экологические и т.д. Легко допустить, что такие «активисты», имей они соответствующие возможности, могли бы охотно атаковать информационно-коммуникационные ресурсы своих оппонентов для нарушения их функционирования, особенно если подобные инциденты будут получать освещение в средствах массовой информации[8].

---

[6] Более подробные данные о современной проблематике кибервойн и защите киберпространства см.: [4].

[7] В состав NCCIC вошли действовавшие ранее независимо Федеральная группа немедленного реагирования на компьютерные инциденты US-CERT (United States Computer Emergency Readiness Team) и Национальный координационный центр телекоммуникаций NCCT (National Coordinating Center for Telecommunications). NCCIC предназначен для координации деятельности и других шести крупнейших федеральных центров кибербезопасности и осуществления тесного сотрудничества с подразделениями Агентства национальной безопасности США, которое стало ядром созданного в июне 2009 г. Объединенного кибернетического командования ВС США (Unified U.S. Cyber Command), ответственного за защиту военного сегмента киберпространства США.

[8] Так, в Объединенном информационно-аналитическом бюллетене от 9 ноября 2007 г., подготовленном управлением МВБ по анализу угроз критической инфраструктуре (DHS/Critical Infrastructure Threat Analysis Division) и подразделением ФБР по анализу угроз (FBI/Threat Analysis Unit) в координации с офисом МВБ по кибербезопасности и коммуникациям, содержалась следующая информация: «В опубликованном на израильском новостном веб-сайте Debkafile сообщении утверждается, что группа, заявившая о своей принадлежности к террористической организации “Аль-Каида”, объявила, что 11 ноября 2007 г. станет первым днем “электронного джихада” в Интернете». В этом же сообщении отмечено, что «неустановленные эксперты в области электроники “Аль-Каиды” намерены с этой даты начать атаки на западные, еврейские и шиитские веб-сайты, а также сайты мусульманских отступников» с последующим подключением к этим атакам все возрастающего числа джихадистских хакеров. Тем не менее МВБ и ФБР не располагают точной и заслуживающей доверия информацией, подтверждающей эти заявления, или разведывательными сведениями, указывающими на связь этой группы с «Аль-Каидой» [25].

По мнению большинства представителей экспертного сообщества США и ряда других развитых стран, особо опасной стороной злоумышленной деятельности в киберпространстве являются попытки вмешательства террористов в функционирование ресурсов, ответственных за управление элементами критической национальной инфраструктуры, за счет неправомерного воздействия на работу автоматизированных систем управления технологическими процессами (АСУ ТП, в зарубежной классификации известных как системы SCADA — Supervisory Control and Data Acquisition), тем более что ряд подобных атак уже получил общественную огласку. Например, еще в 2000 г. не установленный до сих пор злоумышленник дистанционно проник в АСУ городской канализацией австралийского города Маручи Шире и осуществил сброс нескольких миллионов литров неочищенных стоков в протекающую через город реку, что привело к серьезной экологической катастрофе.

Таким образом, в сложившейся современной международной обстановке кибервойны и кибертерроризм стали реалиями, угрожающими нашей цивилизации.

Термин «кибертерроризм» впервые вошел в лексикон специалистов в области национальной безопасности США в 1996 г. Его стали широко применять после его официального включения в «Словарь военных и смежных терминов Министерства обороны США» [12], который фактически устанавливает англосаксонскую военную терминологию, в частности в сфере кибервойн.

Одним из первых фундаментальных исследований в области неправомерного использования киберпространства стал доклад, подготовленный в 1998 г. Центром стратегических и международных исследований CSIS (Center for Strategic and International Studies), под названием «Киберпреступность, кибертерроризм, кибервойны, предотвращение электронного Ватерлоо» [8]. В этом докладе, составленном по итогам широкого обсуждения в экспертном сообществе США и ряда ведущих стран потенциальных последствий подобных атак, были представлены результаты исследования возможности осуществлять указанные действия в киберпространстве, безусловно, способные оказать самое глубокое влияние на жизнедеятельность государства и общества в целом, а также методов ограничения вероятности воплощения такого рода сценариев в жизнь. В этом документе впервые была предложена и трактовка понятия «кибертерроризм».

Кибертерроризм — это преднамеренные политически мотивированные атаки, осуществляемые внегосударственными формированиями, тайной агентурой или даже отдельными людьми, на информационные и компьютерные системы, компьютерные программы и данные в целях нанесения ущерба мирному гражданскому населению.

Несмотря на ясность этого определения, следует оговориться, что одновременно с термином «кибертерроризм» зачастую с подменой понятий некорректно используют термины «кибервойна» и «киберпреступность». Для понятия «кибервойна» все-таки необходимо применять иное определение: **«использование сетевых возможностей одного государства для искажения, нарушения целостности, деградации, манипулирования или уничтожения информации, постоянно находящейся в компьютерах или циркулирующей в компьютерных сетях, или собственно компьютеров и сетей другого государства в целях нарушения цикла разработки и принятия решений»** [22].

Практическая разница между двумя данными терминами состоит в том, что кибертерроризм нацелен на умышленное создание обстановки страха и нервозности среди мирного населения, в том числе нанесение физического ущерба абсолютно случайным людям в зоне проведения террористического акта. Кибервойна имеет вполне конкретную цель вне зависимости от того, идет ли она в рамках войны информационной или реальной.

Наряду с этими двумя терминами существует и понятие «киберпреступность», используемое чаще всего правоохранительными органами. Киберпреступление — это преступление с использованием информационных технологий.

При этом следует подчеркнуть, что **физические формы и методы действий кибертерроризма, кибервойны и киберпреступности зачастую выглядят весьма схоже**.

Яркий пример, демонстрирующий всю сложность разграничения данных понятий, приведен в книге «Кибервойны и кибертерризм», изданной под редакцией известных экспертов в этой сфере Эндрю Коларика и Леха Янчевского: «Представьте себе, что некто получил доступ к медицинской базе данных стационарного лечебного учреждения и изменил медикаментозные назначения конкретному пациенту, уничтожив при этом все данные о его тяжелой аллергической реакции на некоторые типы лекарств. Медицинская сестра, согласно предписанной (но искаженной злоумышленником) схеме лечения, проводит выдачу лекарств, и пациент умирает. Итак, какое определение следует применить? Ответ лежит не в механике самого события, а в намерениях, которые двигали действиями преступника. Если это было сделано умышленно, например вследствие крайне негативных взаимоотношений между этими двумя индивидами, то это — убийство и может по способу исполнения относиться к киберпреступлению. Однако если исполнитель впоследствии намерен предать огласке тот факт, что он готов осуществить гораздо большее количество подобных актов в том случае, если не будут удовлетворены некие его требования, то эти действия могут быть классифицированы как кибертерроризм. Если же данная акция

была проведена тайной агентурой иностранного государства, то это уже операция в рамках кибервойны» [10].

Таким образом, следует подчеркнуть, что **наиболее важной характеристикой кибератаки, приводящей к физическим последствиям, являются намерения атакующего**.

Различия между тремя рассматриваемыми терминами имеют большое значение, поскольку в этой области существуют проблемы и решения, не связанные с технологиями, но оказывающие существенное влияние на любую стратегию противодействия в области кибервойн, кибертерроризма и киберпреступности.

В этой связи попробуем выяснить, 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).

Международно признанного понятия, обозначающего данное явление, не существует, однако есть довольно большое количество частных, зачастую просто ведомственных определений, вытекающих из их целей и задач и поэтому достаточно сильно различающихся.

Трактовка понятия «киберпространство» зависит в первую очередь от того, рассматривается ли оно с точки зрения обеспечения защиты информационно-коммуникационной инфраструктуры государства или с точки зрения ведения военных операций, предусматривающих комплексное и синхронное решение наступательных, оборонительных и специальных, прежде всего разведывательных и упреждающих, задач с использованием всех сил информационных операций. В связи с этим необходимо рассмотреть два определения, трактующих «киберпространство» в узком и широком смысле.

Традиционно, как уже было отмечено, следует обратиться к понятиям, которые дает «законодатель моды» в сфере современных военно-политических терминов — Министерство обороны США. В узком смысле специалисты этого ведомства еще в едином уставе Комитета начальников штабов (КНШ) 2001 г. определили «киберпространство» как «глобальную область в рамках информационного пространства, состоящую из взаимосвязанной сети инфраструктур, созданных на базе информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, а также встроенные в другие технические объекты процессоры и контроллеры» [12]. Однако существует и другая формулировка, которая учитывает комплексный характер любых военных операций и трактует понятие «киберпространство» в более широком смысле. Эта формулировка предложена в едином уставе КНШ ВС США как «сфера

(область), в которой применяются различные радиоэлектронные средства (связи, радиолокации, разведки, навигации, автоматизации, управления и наведения), использующие электромагнитный спектр частот для приема, передачи, обработки, хранения, видоизменения (трансформации) и обмена информации, и связанная с ними информационная инфраструктура ВС США» [13][9].

Фактически первое определение более понятно большинству людей, так как под киберпространством они понимают прежде всего глобальную сеть Интернет, поэтому зачастую в самых различных источниках применяют сформулированную широко известным в мире специалистом в сфере кибербезопасности Томасом Уингфилдом лингвистически более ясную трактовку: «Киберпространство не является материальным местом — оно не поддается никакому измерению в любой физической или временно́й системе мер. Это больше стенографический термин, определяющий пространство, сформированное за счет функционального объединения взаимосвязанных сетей компьютеров, информационных систем и телекоммуникационных инфраструктур, в целом трактуемое как World Wide Web» [26].

Возникновение кибертерроризма как особой формы террористической деятельности, традиционно нацеленного в первую очередь на США и их союзников, во многих случаях является результатом их огромного влияния на современную ситуацию в мире. Соединенные Штаты фактически стали жертвой и заложником парадокса «победы» в «холодной войне» с СССР, а также последующего ведения войн в Югославии, Ираке и Афганистане, а в настоящее время — в Ливии (Сирия на очереди). При этом США позиционируют себя в качестве единственной мировой супердержавы, обеспечивающей поддержание современного миропорядка и распространение «демократических ценностей». Успешность, с точки зрения Вашингтона, военных операций в этих странах в рамках провозглашенной борьбы с международным терроризмом сформировала в мире устойчивое мнение, что любая противостоящая сторона не в состоянии нанести США существенный ущерб, используя традиционные политические, экономические и военные подходы. В результате среди тех, кто продолжает сопротивляться влиянию и давлению Вашингтона, произошло четкое осознание того факта, что единственная возможность достижения своих политических, социальных или экономических целей лежит в способности атаковать США, исполь-

[9] Если принять во внимание эту формулировку, то получившие широкую известность в нашей стране попытки ослепления лазерными лучами экипажей самолетов, заходящих на посадку, с точки зрения американских военных — не просто «лазерное хулиганство», а акты кибертерроризма, поскольку потенциально могут привести к авиакатастрофе и, следовательно, гибели людей.

зуя способы противоборства, отличные от традиционных военных, что в англосаксонской военной терминологии получило название «ведение военных действий другими способами» (WBOM — warfare by other means). Такие действия могут выражаться в двух основных формах.

1. **Кинетические атаки** — непосредственные боевые столкновения противостоящих формирований. Когда противоборствующие силы по своим возможностям несопоставимы, исход традиционной формы противоборства, как правило, приводит к прямому военному поражению более слабой стороны, для которой поэтому наиболее предпочтительными становятся действия непрямого, террористического характера, в частности применение самодельных взрывных устройств непосредственного или дистанционного управления и наиболее эмоционально яркого способа — терактов, осуществляемых террористами-смертниками. При этом очевидно, что стратегически спланированная суицидальная атака может иметь последствия, выходящие далеко за пределы ее прямого оперативного результата. Свой первый весьма чувствительный урок, из которого, правда, так и не были сделаны соответствующие выводы, США получили в Ливане, когда в окрестностях Бейрута была взорвана казарма морской пехоты и погибли свыше 300 морских пехотинцев, а следующим и, безусловно, самым значимым уроком стали теракты 11 сентября 2001 г. в Нью-Йорке и Вашингтоне.

2. **Некинетические атаки** (зачастую рассматриваемые в различных источниках как форма «непрямых действий»). Этот тип атак нацелен не на физическое разрушение, а в первую очередь на процессы выработки и принятия противником решений в политическом и военном аспектах. Традиционно такая форма противоборства выражается в ведении пропагандистской кампании или кампании по дезинформации, успехи и неудачи которых в исторической ретроспективе продолжают вызывать жаркие дискуссии в среде экспертного сообщества не только США, но и многих ведущих стран мира.

Вследствие высокого уровня информатизации всех сторон жизни современного общества в настоящее время основным инструментом некинетических атак становятся информационные операции и их самый чувствительный компонент — операции в киберпространстве. Правда, следует особо подчеркнуть, что некинетические атаки могут иметь и кинетические последствия самого широкого характера, если приводят к принятию противником решений, способных оказать вполне конкретное воздействие на физический, материальный мир.

Безусловно, современная оценка значения некинетических атак не относится к сфере новых концептуальных веяний в военно-политической сфере, поскольку их важность ранее неоднократно

была подчеркнута в различных исследованиях о формах и способах ведения боевых действий.

Так, еще в IV в. до н.э. выдающийся китайский стратег и мыслитель Сунь Цзы в своей нетленной работе «Искусство стратегии» [5] отразил особую значимость воздействия на процесс выработки и принятия решений командующим противника (в современном военном аспекте — на процессы командования и оперативного управления). Сунь Цзы ввел четкую рекомендацию для командного состава любого уровня: «**применять обычные силы для противоборства с противником** [прямой подход], **использовать нестандартность** [непрямой подход] **для победы над ним**» [5, с. 7].

В настоящее время в ряде военных учебных заведений США в обязательную программу входит изучение теоретического наследия другого известного немецкого военного историка и ученого — генерала Карла фон Клаузевица, который в своей работе «О войне» [2] особо подчеркнул важность некинетических воздействий на противника как способа усиления «тумана войны»[10].

Уже в XX в. особое влияние на развитие военной науки ведущих стран мира, прежде всего нацистской Германии, США и Великобритании, оказало фундаментальное военно-теоретическое исследование, состоящее из серии трудов под общим названием «Размышления о войне», автором которого был весьма почитаемый в среде западных военных экспертов английский военный историк и крупнейший военный теоретик Бэзил Лиддел Гарт (Basil Liddell Hart). В этом труде он утверждал: «*Глубочайшая правда войны состоит в том, что исход битвы решается в умах военачальников, а не в телах их воинов*» [17].

Стратегические некинетические атаки прямо нацелены на умы, сердца и процессы выработки и принятия решений военно-политическим руководством противника, поэтому кибервойны и кибертерроризм относятся к очень привлекательным способам ведения некинетических боевых действий. При этом существует ряд факторов, оказывающих определяющее влияние на выбор киберпространства как сферы организации такого способа противоборства [14]:

1) *низкие затраты*. Практически любой пользователь компьютера, имеющего подключение к сети Интернет, может проводить операции в киберпространстве, и стоимость для пользователя будет выражаться всего лишь в оплате услуг доступа к сети и приобрете-

[10] «Туман войны» — военно-теоретический термин (нем. — Nebel des Krieges; англ. — Fog of War). Введен Карлом фон Клаузевицем для обозначения недостоверности данных о положении на театре военных действий в постоянно меняющейся ситуации на поле боя. Применительно к общей обстановке выражает состояние информационной неопределенности, когда командир вынужден принимать решения интуитивно, по наитию и часто вопреки имеющимся данным разведки.

нии программного обеспечения самого разнообразного назначения, в том числе двойного, открыто рекламируемого и продающегося на множестве интернет-сайтов по всему миру. В этой связи потенциальное количество субъектов, способных вести кибероперации против США, подсчитать практически невозможно;

2) *нечеткость традиционных границ*. Операции в киберпространстве способны сформировать свой собственный «туман войны». Учитывая бесконечно большое количество структур самого различного рода, представляющих потенциальную угрозу для США, наличие и коммерческую доступность разнообразных инструментов, способствующих формированию потенциала для проведения кибератак, а также высочайший уровень сформировавшихся взаимосвязей в глобальной сети, зачастую очень сложно вскрыть различия между иностранными и внутренними источниками кибератак. Это приводит к дилемме киберреагирования. Если нельзя определить атакующего, то какой должна быть методика ответа? Внутри США реагирование на киберинциденты осуществляют такие мощные структуры, как МВБ или Киберкомандование ВС США в зависимости от подвергнувшегося атаке сегмента киберпространства — гражданского или военного соответственно. Однако, несмотря на постоянно возрастающие мощь и возможности этих организаций, совершенствование форм и способов их деятельности, раз за разом в официальных пресс-релизах констатируется невозможность установить инициаторов кибератак, получивших широкую огласку в СМИ[11]. При этом если террористическая организация не станет стремиться к формированию собственного потенциала для действий в киберпространстве, а предпочтет нанять третью сторону, то проблема еще более обострится;

3) *повышенная значимость для управления общественным мнением*. Многие террористические организации, а также активистские структуры, противостоящие США, в настоящее время уже обладают возможностями без особых усилий манипулировать общественным мнением за счет производства и размещения во Всемирной сети различного рода цифровой информации или внесения изменений в мультимедийные файлы. При этом следует особо подчеркнуть, что в использовании киберпространства не существует оперативных пауз, традиционно характерных для организации противоборства в других сферах (на суше, море, в воздухе и космосе)[12], оно

[11] Чаще всего вскрытие и арест участников кибератак происходят при осуществлении ими киберпреступлений в финансовой сфере, когда, например, при проведении незаконных транзакций финансовых средств удается вскрыть маршрут перевода денег и пункт их получения.

[12] Опубликованная в марте 2005 г. Стратегия национальной обороны США отнесла киберпространство к новому театру военных действий [6].

доступно круглосуточно, поэтому в задачу управления общественным мнением входит и адекватное противостояние негативному влиянию на него. Реагирование, как правило, всегда более затратно по ресурсному обеспечению. Отсутствие противодействия негативному влиянию на формирование общественного мнения может дискредитировать первоначальный замысел любой операции или привести к непосредственному прекращению миссии, если эти усилия не стали успешными. Например, американское участие в операции в Сомали в период с 1992 по 1994 г. привело именно к таким результатам. Все усилия администрации президента У. Клинтона стали тщетными, когда они не смогли противостоять формированию негативного общественного мнения внутри своей страны после размещения в Интернете фотографий крайне изувеченного американского военнослужащего, труп которого, привязанный к автомобилю, волокли по улицам Могадишо;

4) *сложность ведения стратегической разведки*. Традиционные методы сбора разведывательной информации и соответствующие аналитические технологии в отношении киберпространства в основном устарели. Размывание традиционных границ — существенный фактор в этой проблеме. Поскольку практически каждый пользователь сети может использовать Интернет в любое удобное для него время и с необходимой ему продолжительностью подключения, террористы также могут развернуть и свернуть свои центры организации кибератак гораздо быстрее, чем органы и силы защиты национального киберпространства будут в состоянии идентифицировать их и оценить их намерения;

5) *сложность тактического оповещения и оценки атаки*. Вследствие простоты и коммерческой доступности инструментов для проведения кибератак и того факта, что практически любой пользователь сети может их инициировать, отличить обычный поиск информации от атаки соответствующих структур другого государства или террористической структуры в реальности весьма затруднительно. Соответственно, США могут не знать, когда атака началась, каким образом она осуществляется и кем. Возможно, анонимная сущность киберпространства и будет преодолена со временем, но пока в момент начала противоборства успех сопутствует атакующему;

6) *трудность в формировании и поддержании коалиции*. Проведение коалиционных военных операций является непреложным приоритетом США практически в любой военной кампании. Однако общая сетевая безопасность коалиции реализуема лишь тогда, когда между партнерами существуют устойчивые сетевые связи и единые стандарты, формы и способы ее поддержания. При их отсутствии или несогласованности менее технологически развитые партнеры могут представлять собой потенциальный «черный вход» в инфор-

мационные системы Соединенных Штатов. Необходимость модернизации коалиционной системы сетевой безопасности и устранения факторов, способствующих выбору некоторых членов коалиции в качестве потенциальных целей, накладывает на Вашингтон обязанности по вложению существенных ресурсов как в настоящее время, так и на перспективу;

7) *уязвимость национальной территории США*. Современные исследования отражают тот факт, что Соединенные Штаты в своем развитии во все большей степени будут зависеть от комплексных, взаимосвязанных и объединенных сетями передачи данных информационных систем, тем самым предоставляя потенциальным злоумышленникам богатое разнообразными целями пространство. При этом уязвимость по отношению к кибератакам будет только возрастать вследствие того факта, что средства нападения, как правило, всегда опережают средства защиты.

Современные затраты, требуемые для проведения кинетических атак традиционного типа, для потенциальных оппонентов Вашингтона слишком высоки, если не сказать неподъемны, вследствие несопоставимости их возможностей с возможностями США, при этом они только косвенно могут затронуть военные, физические и экономические аспекты общества.

В связи с этим, по мнению большинства членов экспертного сообщества США, единственный путь, который может оказаться более или менее результативным для сил, противостоящих Соединенным Штатам, — это «ведение военных действий другими способами». Только некинетические атаки, в первую очередь в рамках кибервойны, способны затронуть территорию США в политическом и социальном, а также военном, физическом и экономическом аспектах.

В отношении собственно форм и способов действий террористов в киберпространстве уже более двух десятков лет дискуссии в экспертном сообществе США и их ближайших союзников остаются весьма напряженными. При этом исследователи в этой области сталкиваются с теми же проблемами, что и при изучении традиционного терроризма. Главная трудность состоит в том, что международное сообщество до сих пор не выработало общепринятого определения кибертерроризма. Зачастую в США наряду с формулировкой CSIS, предложенной еще в 1998 г., используют следующую трактовку: «Противоправное уничтожение, дезинтеграция или дезинформация цифровой собственности (имущества) в целях устрашения или принуждения государства или общества для достижения целей политического, религиозного, идеологического или иного характера» [7].

Главное отличие этого определения от выработанного CSIS состоит в том, что оно сосредоточено на манипуляции цифровой собственностью. Пока еще не было никаких доказательств, что кибертерроризм (не имеются в виду известные случаи межгосударственных кибервойн) может оказывать какое-либо прямое воздействие на физическое имущество или людей. Кибертерроризм по своей сути 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. В предшествующей части этой статьи отмечено, что наступательные операции в киберпространстве с применением кибероружия, а следовательно, и кибертерроризм могут привести к кинетическим эффектам.

В определении, данном в едином уставе КНШ ВС США [13], подчеркивается, что операции в киберпространстве являются потенциальным усилителем обычных сил, поэтому и террористы могут использовать киберпространство для поддержки проведения обычных террористических операций. Эту деятельность специалисты по информационным операциям ВС США трактуют так: «Противоправное использование информационно-коммуникационных систем террористом или группой террористов, которое само по себе не предназначено для насильственных воздействий в отношении целевой аудитории. Кибертерроризм в данном случае нацелен на поддержку и усиление результативности традиционных террористических акций» [24].

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.

Не все кибератаки планируются и осуществляются одинаково, поскольку не все террористы имеют одинаковые возможности, да и цели их различны. Технический анализ потенциальных кибератак, по оценке некоторых специалистов США в этой области [14], позволяет разделить их на три широких класса.

1. **Простая неструктурированная атака** (simple unstructured attack) — атака начального уровня в отношении отдельных систем с использованием программно-технических средств, разработанных чаще всего непричастными к терроризму лицами.

Основной целью при этом является нарушение или замедление функционирования объекта атаки. Как правило, ее инициаторы имеют низкие возможности по анализу цели, невысокий уровень организации и инженерно-технической подготовки. Подобные атаки наиболее распространены в современном Интернете. Как правило, террорист скачивает из Всемирной сети подходящие хакерские программы и применяет их в отношении намеченной цели. Атака весьма ограничена по времени и последствиям. Если в системе установлены адекватные средства обеспечения кибербезопасности, то такая атака отражается достаточно просто, при этом восстановление системы требует минимальных усилий.

2. **Усложненная структурированная атака** (advanced structured attack) — более сложная атака в отношении множества систем или сетей с проведением модернизации или разработки базового хакерского программного обеспечения. При этом инициатор атаки (организация или отдельное лицо) в состоянии проводить элементарный анализ цели и структуры управления для осуществления серии атак из единственной точки дислокации, самостоятельно обучаться, осваивать новые технологии, распространять их и обучать других.

Главная цель атакующего состоит в нарушении и нейтрализации операционной функциональности объекта атаки. Ее инициатор обладает более высоким уровнем киберподготовки и образования, чем террорист, который может осуществить только простую неструктурированную атаку, возможностями проводить разведку в целях вскрытия специфических уязвимостей объекта и оценки его конкретного функционального предназначения, а также порядка проведения операций. На этом уровне атакующий не просто заимствует находящееся в свободном доступе программное обеспечение, но и самостоятельно проводит его модификацию. Возможности по организации атак этого уровня отражают прежде всего тот факт, что террорист входит в состав более крупной и хорошо обеспеченной ресурсами террористической структуры, цели которой могут не ограничиваться только киберпространством. Усилия по восстановлению функциональности объекта после атак данного уровня требуют существенных затрат времени и ресурсов. При этом организация защиты от таких атак не потребует слишком больших усилий в освоении технологий киберзащиты и обучении обслуживающего персонала.

3. **Комплексная скоординированная атака** (complex coordinated attack) — высший уровень. Ее проведение позволяет осуществить координацию кибератак, цель которых состоит в массовом уничтожении или дезинтеграции данных. На исполнение атак этого типа способна только организация, а не отдельный человек. При этом

атакующая структура обладает очень высоким уровнем возможностей по анализу уязвимостей объекта (цели), обеспечению прорыва интегрированной многоуровневой системы защиты и разработке уникального, высокотехнологичного программного обеспечения для проведения атак. Такая организация имеет мощную и гибкую структуру управления, способную осуществлять множественные и синхронизированные атаки из различных мест киберпространства. Это строго ориентированная на знания организация, состоящая из профессионалов, способных создать кибероружие собственной разработки, доктрины и организационные структуры.

Оперативным примером способностей таких групп может быть массированная атака на национальную сеть телефонной связи или другие элементы критической инфраструктуры государства. В реальности же этот тип кибератак выходит далеко за рамки возможностей подавляющего большинства, если не абсолютно всех существующих на сегодня типичных террористических групп. Этот вывод не относится, тем не менее, к государствам, которые, по мнению некоторых ведущих экспертов США, могут использовать кибертерроризм как форму «ведения военных действий другими способами».

Кибератаки этого уровня относятся к исключительно высокотехнологичным, при этом вероятность их проведения до появления программного вируса «Stuxnet» рассматривали как весьма низкую, поскольку для этого необходим высочайший уровень квалификации и затрачиваемых ресурсов. Успешно проведенная атака такого типа может иметь крайне разрушительные последствия и ощущаться на государственном уровне, как это случилось в Иране. Усилия по восстановлению могут быть крайне затратными по времени и ресурсам.

Следует учитывать еще один аспект проблемы кибертерроризма. Фирма «Symantec» утверждает, что на разработку вируса «Stuxnet» потребовалось 6—9 месяцев работы команды в составе 5—6 специалистов. Это означает, что мощная и хорошо обеспеченная ресурсами террористическая организация, если у нее нет таких профессионалов, способна найти их и привлечь за приличное финансовое вознаграждение к выполнению разработки подобного типа. Такой подход ничем не будет отличаться от попыток террористических структур создать или приобрести оружие массового поражения или его компоненты, как это произошло в случае неорелигиозной организации «Аум Синрикё», которая получила доступ к боевому отравляющему веществу (нервно-паралитическому газу зарину) и применила его в террористической атаке 20 марта 1995 г. в токийском метро, что привело к многочисленным человеческим жертвам.

Определив потенциальные способы и формы организации атак кибертеррористов, все-таки необходимо задаться вопросом: «А сами

террористы заинтересованы рассматривать атаки в киберпространстве в качестве оперативного метода?».

С одной стороны, Всемирная сеть предоставляет практически любому человеку возможности дистанционного доступа к глобальным целям, а учитывая все возрастающую зависимость всех сторон жизни современных западных обществ от компьютерных технологий, кибертерроризм можно рассматривать как весьма эффективную форму асимметричной борьбы. При этом, по иронии, отсутствие мирового консенсуса по вопросу о том, что считать актом кибертерроризма, предоставляет инициаторам кибератак определенный уровень юридической защищенности, полностью отсутствующей в случае проведения актов физического террора. Кроме того, 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.

С другой стороны, существует и множество преград для использования киберпространства обычными террористами в террористических целях, ведь большинство экстремистских группировок, как и любые другие организации, если за ними не стоит поддерживающее их деятельность государство, как правило, обладают ограниченными ресурсами.

Несмотря на то что затраты на проведение операций в киберпространстве обычно низкие, такие атаки могут не достичь желаемых стратегических целей организации. Это касается в первую очередь террористических групп, нацеленных на физическое уничтожение материальных средств и гибель людей. Кроме того, 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 этот фактор, 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.

Решение использовать или не использовать кибертерроризм в качестве активного метода противоборства зависит также от типа террористической группы, ее целей и задач. Проведение операций

в киберпространстве может просто им не соответствовать. Например, террористические группы религиозного толка могут отказаться от применения кибертеррора, возможно, только потому, что его результаты не приводят к человеческим жертвам, разрушениям или не находят желаемого отклика в средствах массовой информации. Напротив, организации, нацеленные на подрыв коммерческой деятельности крупных бизнес-корпораций, все чаще прибегают к проведению актов кибертеррора. Так, по результатам исследования, проведенного фирмой «Symantec» в 2010 г. и посвященного защите критической инфраструктуры от киберугроз с обобщением данных опроса сотрудников 1580 компаний из 15 стран мира, чуть больше половины (53%) респондентов подтвердили свои подозрения о том, что их компании уже были объектами атак, преследовавших конкретные политические цели, причем, по оценкам самих компаний, за последние 5 лет они подвергались кибератакам около 10 раз. Еще 48% опрошенных были уверены, что их организации станут объектами атаки в течение ближайшего года. Подавляющее же большинство (80%) респондентов посчитали, что частота таких атак увеличивается и эффективность их остается высокой. По их (усредненной) оценке, 3 из 5 кибератак являются успешными [3].

Место базирования террористической группы и регион ее операций также являются существенными факторами. Проведение кибератак просто невозможно, если отсутствует устойчивый доступ к технологическим ресурсам. Например, группа, базирующаяся в джунглях Перу, с ограниченным доступом к Интернету вряд ли будет заниматься кибертерроризмом, в отличие, например, от группы, дислоцированной в ФРГ и широко использующей Всемирную сеть.

Иными словами, уровень технических возможностей может в итоге стать решающим фактором при выборе террористической организацией киберпространства как оперативной сферы своей деятельности. При этом технические навыки не являются критическим ограничителем для осуществления атак самого простого уровня. Навыки и опыт становятся весьма важным аспектом в том случае, если группа планирует осуществить атаки среднего уровня (усложненные структурированные) или высшего (комплексно скоординированные).

В соответствии с руководящими документами, директивами, уставами и наставлениями МВБ и ВС США все наступательные операции в киберпространстве, неважно с чьей стороны они проводятся, попадают под одну из трех категорий: уничтожение, дезинтеграция или дезинформация [16]. Кибероперации, приводящие к уничтожению материальных средств, до осени 2010 г. не относились к категории реальности, поскольку до появления программного вируса «Stuxnet», вредоносной программы для операционной

системы Windows, разработанной для нарушения работы и перепрограммирования крупномасштабных промышленных компьютерных систем, не было отмечено ни одного инцидента физического разрушения, наступившего вследствие применения компьютерного вируса или проведения какой-либо иной формы кибератаки. Безусловно, многие эксперты в области компьютерной безопасности не отрицали, что такие возможности могут быть созданы в отдаленном будущем, но при этом подчеркивали крайне низкую вероятность того, что даже самые технологически развитые оппоненты США будут в состоянии разработать такие возможности хотя бы в среднесрочной перспективе.

Применение вируса «Stuxnet» произвело эффект разорвавшейся бомбы, когда в сентябре 2010 г. сообщения о зараженных иранских промышленных предприятиях, прежде всего в ядерной сфере, стали главной новостью всех основных средств массовой информации [4, с. 5]. Чуть позже аналогичные системы в России и Казахстане также испытали значительные трудности вследствие воздействия данной программы.

Если ранее большинство случаев злоумышленных вирусных атак были мотивированы возможным финансовым вознаграждением или нарушением общего характера функционирования сетевой структуры, то вирус «Stuxnet», несомненно, был разработан для поражения критической инфраструктуры. Самая важная его характеристика состоит в том, что он может воздействовать на внешние программируемые логические контроллеры (ПЛК) и распространяться через переносные носители информации на компьютерах, не подключенных к Интернету, а также обходить технологию HIPS (Host Intrusion Prevention System), которая защищает от попыток внешнего воздействия на систему. Это стало возможным благодаря наличию во вредоносной программе файлов, имеющих легальные цифровые подписи [11].

Данный случай, по мнению большинства членов мирового экспертного сообщества, перевел нашу цивилизацию в новую эру, в которой кибервойны и применение кибероружия, нацеленного на разрушение критической инфраструктуры, больше не относятся к абстрактной категории. При этом вирус «Stuxnet» был признан экспертами в области кибервойн как первое реальное кибероружие. Вторым подобным случаем, возможно, стоит назвать атаку вируса «Stars» на иранские промышленные и военные объекты в апреле 2011 г., о чем заявил начальник подразделения пассивной обороны Ирана Голам Реза Джалали, правда, конкретных данных об этом вирусе со стороны ведущих фирм в области кибербезопасности не отмечено [21].

Евгений Касперский, видный отечественный специалист и основатель мощного бизнеса в сфере обеспечения безопасности Ин-

тернета под названием «Лаборатория Касперского», чье мнение весьма авторитетно, чуть позже, комментируя этот киберинцидент в своем выступлении на конференции в Мюнхене, заявил: «Я боюсь, что это начало нового мира. 1990-е годы были десятилетием кибервандалов, 2000-е были десятилетием киберпреступности. Я боюсь, что сегодня наступила новая эра — эра кибервойн и кибертерроризма» [11].

Пока случаи уничтожения материальных средств исключительны и единичны, и за ними, скорее всего, стоят мощные государственные структуры, но дезинтеграция в настоящее время остается наиболее реальной и распространенной формой ведения наступательной кибервойны. Этот тип операций может быть наиболее наглядно продемонстрирован на примере искажения содержимого веб-страниц, распространения компьютерных вирусов и других программных атак, нацеленных на повреждение критических данных в системах обработки информации. Уровень технологической сложности, необходимый для проведения этого типа атак, весьма незначителен. Специализированные программы можно легко найти в Интернете, при этом практически любой пользователь среднего уровня в состоянии их скачать и применить. Желательный результат таких операций состоит в том, чтобы лишить противника (как минимум временно) использования его информационных систем и добиться расходования ценных ресурсов на их восстановление [1].

Дезинформация представляет собой тщательно спланированную манипуляцию информацией для воздействия на формирование общественного мнения. Целью этой операции является создание такого враждебного общественного климата, который способен повлиять на политику противника в нужном для атакующего русле. Дезинформация отличается от двух других форм наступательных операций тем, что ее цель — не только собственно противоборствующая сторона, но и те сторонние силы, которые способны оказать непосредственное влияние на ее позицию.

Один из главных недостатков этого типа операций состоит в том, что при проведении атаки должны быть согласованы все более или менее точные детали, поскольку разоблачение источника дезинформации может привести к непредсказуемой реакции по отношению к злоумышленнику и консолидации в поддержке атакованного.

Оборонительные операции в киберпространстве применяются в рамках любого возможного спектра военных и невоенных операций, при этом главной их целью является формирование необходимых мер по защите и обороне ключевой критической инфраструктуры. Эффективные оборонительные кибероперации необходимо проводить максимально широко и по всей глубине защиты, до самого низкого возможного уровня.

Для США, как и для других стран, существуют четыре главные задачи в области кибероборонь. Первая состоит в формировании защищенного киберпространства. Поддержание высокого уровня защиты позволяет сохранять свободу в использовании информационно-коммуникационных систем, когда и где это будет необходимо. Вторая относится к проблеме вскрытия атаки. Как было отмечено ранее, одна из главных причин привлекательности кибервойн как формы непрямого противоборства состоит в формировании собственного «тумана войны». Системы, не сконфигурированные должным образом или со слабым системным администрированием, могут даже не почувствовать, что являются объектом атаки. Третья задача состоит в необходимости обеспечить быстрое и эффективное восстановление систем, подвергнувшихся нападению, чтобы свести к минимуму возможные потери. Четвертой и конечной задачей является реагирование на саму атаку.

Оборонительные и наступательные кибероперации, безусловно, относятся к взаимоподдерживающим. Хорошо организованные оборонительные операции могут помочь вскрыть источник атаки, что позволяет впоследствии провести наступательную операцию возмездия по конкретной цели.

Оборонительные операции разрабатываются для обеспечения гарантии конфиденциальности, целостности, доступности, безотказности и аутентичности своих и союзных систем. В представленной таблице обобщены основные признаки каждой из указанных категорий.

Краткие характеристики категорий оборонительных операций в киберпространстве

Категория	Краткая характеристика
Конфиденциальность	Действия, направленные на воспрепятствование доступа к информации несанкционированным пользователям
Целостность	Действия, направленные на поддержание целостности информации за счет предотвращения несанкционированного создания, изменения или уничтожения данных
Доступность	Действия, направленные на обеспечение легитимным пользователям гарантированного доступа к информационно-вычислительным ресурсам, включая собственно информацию, обработку и обеспеченность связью
Безотказность	Действия, направленные на исключение возможности одной из сторон в системе связи впоследствии ложно обвинить систему в том, что сеанс коммуникации не состоялся
Аутентичность	Действия, направленные на обеспечение гарантированной идентификации участников операции в системе

Следует также отметить, что, по оценке Министерства обороны США, наступательные и оборонительные операции в киберпространстве являются ключевыми элементами информационных операций (информационного противоборства). Они предназначены для поддержки решения всего спектра задач в сфере обеспечения национальной безопасности. В мирное время операции в киберпространстве наряду с другими элементами национальной мощи направлены на предотвращение конфликтов, во время кризиса они позволяют склонить ситуацию в пользу США и помочь избежать потенциальной эскалации. В период конфликта активное использование киберпространства может стать усилителем действий кинетических сил, направленных на одержание победы над противником, и оказать помощь в переходе к операциям по стабилизации обстановки мирного времени [15].

* * *

Таким образом, рассмотрев побудительные мотивы террористов в использовании киберпространства как оперативного поля для своей деятельности, потенциальные способы организации кибератак как формы «непрямых действий» и «ведения военных действий другими способами», необходимо подчеркнуть, что кибертерроризм не относится к вымышленным понятиям, это реальная и серьезная угроза, тем более что кибератаки на простом и среднем уровнях осуществляются в сети Интернет регулярно. В США же, несмотря на беспрецедентные меры в сфере противодействия терроризму, принятые после терактов 11 сентября 2001 г., в том числе в области кибербезопасности, возможность наступления «цифрового Перл-Харбора» не исключена, и Вашингтон ясно осознает эту опасность.

СПИСОК ЛИТЕРАТУРЫ

1. Иранские хакеры напугали правительство Нидерландов [Электронный ресурс] // Вести.ru [Офиц. сайт]. 04.09.2011 г. URL: http://www.vesti.ru/doc.html?id=559086 (дата обращения: 27.08.2011).

2. *Клаузевиц К.* О войне. М.: Римис, 2009.

3. Критическая инфраструктура оказалась в киберопасности [Электронный ресурс] // Business FM [Офиц. сайт]. 17.11.2010 г. URL: http://www.bfm.ru/articles/2010/11/17/kriticheskaja-infrastruktura-okazalas-v-kiberopasnosti.html (дата обращения: 25.08.2011).

4. *Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А.* Кибервойны — реальная угроза национальной безопасности? / Институт проблем международной безопасности РАН; Факультет мировой политики МГУ имени М.В. Ломоносова. М.: КРАСАНД, 2011.

5. *Сунь Цзы.* Искусство стратегии. М.: Эксмо, 2009.

6. *Alexander K.B.* Warfighting in Cyberspace. Joint Forces Q., July 31, 2007 [Electronic resource] // Military.com [Web portal]. URL: http://www.military.com/forums/0,15240,143898,00.html (accessed: 21.08.2011).

7. *Bohannon L.* Cyberspace and the New Age of Influence. School of Advance Air and Space Studies. Maxwell AFB, Alabama: Air University, June 2008.

8. Center for Strategic and International Studies. Cybercrime, Cyberterrorism, Cyberwarfare, Averting Electronic Waterloo. Washington, D.C.: CSIS Press, 1998.

9. Critical Infrastructure and Key Resources Sectors [Electronic resource] // Department of Homeland Security [Official website]. URL: http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/sectorMenu.htm (accessed: 14.01.2011).

10. Cyber Warfare and Cyber Terrorism / Ed. by A. Colarik, L. Janczewski. N.Y., 2008.

11. *De Silva R.* Stuxnet Cometh: Defense Agencies Prepare for Next Generation Warfare, October 27, 2010 [Electronic resource] // Defense IQ [Web portal]. URL: http://www.defenceiq.com/defence-technology/articles/stuxnet-cometh-defence-agencies-prepare-for-next-g/ (accessed: 21.08.2011).

12. Joint Chiefs of Staff, Joint Publication 1-02, Department of Defense Dictionary of Military & Associated Terms (April 12, 2001) [Electronic resource] // Defense Technical Information Center [Official website]. URL: http://www.dtic.mil/doctrine/jel/newoubs/jp102.pdf (accessed: 25.08.2011).

13. Joint Chiefs of Staff, Joint Publication 3-13. Information Operations. February 13, 2006 [Electronic resource] // Defense Technical Information Center [Official website]. URL: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed: 25.08.2011).

14. *Molander R.C.* Strategic Information Warfare. A New Face of War. Santa Monica, CA: Rand Corporation, 1996.

15. *Nelson B.* Cyberterror, Prospects, and Implications. Monterey, CA: Center for the Study of Terrorism and Irregular Warfare; Naval Post Graduate School, 1999.

16. *O'Hara T.F.* Cyber Warfare / Cyber Terrorism. USAWC Strategy Research Project, U.S. Army War College, March 19, 2004 [Electronic resource] // Defense Technical Information Center [Official website]. URL: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA424310 (accessed: 25.08.2011).

17. *Parks R.C., Duggan D.P.* Principles of Cyber-Warfare. Paper presented at the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, N.Y.

18. Potential Indicators of Terrorist Activity, Infrastructure Category: Chemical Storage Facilities. Protective Security Division, Department of Homeland Security, Draft Version 1, January 30, 2004 [Electronic resource] // Department of Homeland Security [Official website]. URL: http://www.dhs.gov/dhspublic/index.jsp (accessed: 28.08.2011).

19. Potential Indicators of Terrorist Activity, Infrastructure Category: Highway Tunnels. Protective Security Division, Department of Homeland Security, Version 2, September 22, 2003 [Electronic resource] // Department of Homeland Security [Official website]. URL: http://www.dhs.gov/dhspublic/index.jsp (accessed: 28.08.2011).

20. Potential Indicators of Terrorist Activity, Infrastructure Category: Petroleum Pipelines. Protective Security Division, Department of Homeland Security, Draft Version 1, March 5, 2004 [Electronic resource] // Department of Homeland Security [Official website]. URL: http://www.dhs.gov/dhspublic/index.jsp (accessed: 28.08.2011).

21. *Rashid F.Y.* Iran Claims Stars Virus a Second Cyber-Attack [Electronic resource] // Eweek.com [Web portal]. April 25, 2011. URL: http://www.eweek.com/c/a/Security/Iran-Claims-Stars-Virus-a-Second-CyberAttack-726573 (accessed: 21.08.2011).

22. *Schaap A.J.* Cyber Warfare Operations: Development and Use under International Law // Air Force Law Review. Vol. 64. Winter, 2009. P. 121—174.

23. Ten-Year Anniversary of 9/11 Attacks: No Specific Threats, but a Potentially Attractive Terrorist Target: Joint Intelligence Bulletin. August 10, 2011 [Electronic resource] // Public Intelligence [Web portal]. URL: http://info.publicintelligence.net/DHS-FBI-911-Anniversary.pdf (accessed: 28.08.2011).

24. *Thomas T.L.* Cyber Silhouettes: Shadows Over Information Operations. Foreign Military Studies Office, Fort Leavenworth, KS, 2005.

25. Unsubstantiated Threat of Al-Qa'ida "Electronic Jihad" on 11 November 2007. Joint Intelligence Bulletin, November 9, 2007 [Electronic resource] // Public Intelligence [Web portal]. URL: http://info.publicintelligence.net/DHS-ElectronicJihad.pdf. (accessed: 01.06.2011).

26. *Wingfield T.C.* The Law of Information Conflict: National Security Law in Cyberspace. Aegis Research Corporation, 2000.