Раздел 2. Преступления террористического характера в разных сферах деятельности

В.А. Номоконов, доктор юридических наук,профессор,

Т. Л. Тропина

Терроризм с помощью Интернета

Развитие новых информационных технологий с их простотой доступа, относительно низкой стоимостью и широкомасштабностью открывает терроризму новые границы и обусловливает появление такой новой и опасной его разновидности как кибертерроризм. Данный процесс заметно ускорился в связи с существенным расширением сферы Интернета.

По прогнозам специалистов, к 2005 г. к глобальной сети Интернет будет подключено более 1 млрд. компьютеров. Уже сегодня в Интернете размещено несколько миллиардов сайтов. Ежеквартально объем передаваемых через Интернет данных удваивается и можно уверенно говорить о появлении реальной зависимости большинства стран от надежности функционирования международной информационной инфраструктуры[1].

Кибертерроризм проявляется во вмешательстве в работу компонентов телекоммуникационных сетей, функционирующих в их среде компьютерных программ, несанкционированной модификации компьютерных данных, что вызывает дезорганизацию работы т.н. критически важных элементов инфраструктуры государства и создает опасность гибели людей, значительного имущественного ущерба или иных тяжких последствий. От обычного хакерства данный вид терроризма отличается прежде всего целями и мотивами, а также размерами причиняемого ущерба. Так, согласно Акту Патриота США (2001 г.), к последнему отнесены «различные квалифицированные формы хакерства и нанесения ущерба защищенным компьютерным сетям граждан, юридических лиц и государственных ведомств на совокупную сумму, равную и превышающую 5 тысяч долларов, включая ущерб, причиненный компьютерной системе, используемой государственным учреждением при организации национальной обороны или обеспечении национальной безопасности» (ст. 814).

Кибертерроризм представляет собой серьезную опасную угрозу для человечества, по оценкам специалистов сравнимую с ядерным,

---

[1] http://www.crime-research.ru

[1] См.: Голубев В. Электронный терроризм - новое лицо терроризма // http://www.crime-research.ru. Впрочем., существуют и иные оценки, согласно которым риск кибертерроризма завышен. См. подробнее: Lewis J. Assesing the Risks of Cyber Terrorizm, Cyber War and Other Cyber Threats (2002).

бактериологическим и химическим оружием, причем степень этой угрозы – в силу своей новизны – не до конца еще осознана. Кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара. По данным ООН, мировые убытки от преступлений, связанных с использованием компьютеров, уже превысили 1 трлн. долл. США. Особую озабоченность среди специалистов вызывает уязвимость компьютерных систем управления критической инфрастуктурой (транспорт, атомные электростанции, водоснабжение и энергетика), подключенных к Интернету[1].

В этой связи отметим, что в мире сегодня заметно обострилась проблема использования информационного оружия, пока не ограниченного никакими нормами международного права. Разработки таких средств ведутся уже в 120 странах (в то время как ядерного оружия - лишь в 20)[2].

Угроза кибератак является вполне реальной и связанные с ней риски оцениваются специалистами как высокие. С точки зрения экспертов и правоохранительных органов, наибольшая угроза со стороны кибертеррористов заключается в предоставляемых им возможностях глобальной информационной сети Интернет для осуществления кибератак, направленных на уязвимые звенья критической инфраструктуры, в первую очередь, транспорта и энергетики[3].

По сообщению Министерства национальной безопасности США, недавно были задержаны некоторые активисты из террористической организации «Аль-Каида», деятельность которых представляла опасность для Соединенных Штатов. В результате допросов задержанных удалось узнать, что «Аль-Каида» продолжает планирование террористических актов против США. Так, были названы главные мишени террористов - энергетика и транспорт. 4 сентября 2003 года Министерство национальной безопасности США сделало предупреждение о возможности нападения кибертеррористов. Одним из пунктов в списке возможных действий террористов было применение информационных технологий с использованием Интернет в качестве орудия совершения террористических актов[4].

Террористам любого масштаба – как новичкам, так и профессионалам – Всемирная сеть предлагает средства доступа к огромной аудитории. Если в прошлом террористические группы были вынуждены использовать традиционные средства массовой информации (в результате чего распространение ее было все-таки значи-

---

[2] См: Смирнов А.И. Некоторые проблемы информационной безопасности в международных отношениях // Информация. Дипломатия. Психология. М., 2002. С. 352.
[3] См: http://www.crime-research.ru
[4] Там же.

тельно легче нейтрализовать), то теперь любой пользователь сети может получить последнюю информацию о деятельности различных террористических организаций.

Интернет предоставляет прекрасные возможности тем, в чью задачу входит координирование деятельности групп единомышленников в труднодоступных местах, - этим, разумеется, не могли не воспользоваться террористические организации. Например, Бен Ладен использовал киберпространство для оказания информационной поддержки соотечественникам в Египте, являющимся ветеранами войны в Афганистане. Электронные доски объявлений, электронная почта, интерактивное общение использовались организацией Аль-Каида для поддержания связи с группировками Хамас и Хезболлах[1]. Но это лишь малая часть тех возможностей, которые дает террористам использование World Wide Web. Способы использования террористами сети Интернет весьма разнообразны. С помощью Интернета осуществляются:

1. Сбор подробной информации о предполагаемых целях, их местонахождении и характеристике.
2. Сбор денег для поддержки террористических движений. Так, например, сайт о Чеченской республике представляет номер счета банка в Калифорнии, на который можно перечислить средства для поддержки чеченских террористов.
3. Создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени и встрече людей, заинтересованных в поддержке террористов, указаний о формах протеста и т.п., т. е. синергетическое воздействие на деятельность групп, поддерживающих террористов.
4. Вымогательство денег у финансовых институтов с тем, чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию.
5. Использование Интернета для обращения к массовой аудитории для сообщения о будущих и уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте, а также предание террористами с помощью Интернета широкой гласности своей ответственности за совершение террористических актов.
6. Поскольку «электронам не надо предъявлять паспорт»[2], терроризм не ограничен больше тем государством, где скрываются террористы, более того, базы подготовки террористических опера-

[1] Подробнее см.: Современная проблема международной киберпреступности // Борьба с преступностью за рубежом. 2001. № 2. С. 18.
[1] Denning D. E. " Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" http://www.nautilus.org/info-policy/workshop/papers/denning.html

ций уже, как правило, не располагаются в тех странах, где находятся цели террористов.

7. Если раньше сеть террористов обычно представляла разветвленную структуру с сильным центром, то теперь это сети, где не просматривается четких командных пунктов, более того, могут быть ничего не подозревающие соучастники – например, хакеры, которым неизвестно, к какой конечной цели приведут их действия.

8. «Всемирная паутина» может инициировать психологический терроризм. С помощью Интернета можно посеять панику, ввести в заблуждение, привести к разрушению чего-либо. Всемирная сеть – благодатная почва для распространения различных слухов, в том числе и тревожных. Так, 5 ноября 2003 г. «Аль Каида» распространила через Интернет предупреждение всем мусульманам, проживающим в трех крупнейших городах США, о необходимости немедленно покинуть эти города в связи с предстоящим новым терактом[1].

9. Как уже было сказано выше, возможности электронной почты или электронных досок объявлений используются для отправки зашифрованных сообщений.[2]

К вышеперечисленным способам можно добавить также размещение в Интернете сайтов террористической направленности, содержащих информацию о взрывчатых веществах и взрывных устройствах, ядах, отравляющих газах, а также об их самостоятельном изготовлении. Только в русскоязычном Интернете десятки сайтов, на которых можно найти подобные сведения.

Терроризм в сети позволяет не только атаковать глобальные цели или готовиться к таким атакам, он также дает возможность проводить террористические акции без физического присутствия исполнителей[3].

Сейчас иной раз говорят о концепции «бескровного терроризма», т. е. о возможности такого вида террористических актов нанести огромный экономический ущерб без причинения вреда человеческой жизни. Но вряд ли этой концепции придерживаются такие террористические группировки, как Аль-Каида, Тигры освобождения Тамила, Курдская рабочая партия, испанская ЕТА, способные использовать опасные вирусы или другие формы кибернетического воздействия для нападения на службы неотложной медицин-

---

[1] См. подробнее: Макарычев М. «АльКаида» подала голос // Рос. газета. 2003. 6 ноября.

[2] Подробнее о перечисленных способах см.: Томас Тимоти Л. Сдерживание ассиметричных террористических угроз, стоящих перед обществом в информационную эпоху // Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции. М., 2002.

[3] Так, вирус Love Rug пришел с Филиппин, хотя, как утверждают, его источники находятся в Германии. Кибернападения на США и Европу вполне может быть проведено террористами из Ливана, Судана, Йемена. Вирус Blaster причастен к «всеамериканскому энергозатмению», а его виртуальный противник Welchia умудрился 23 сентября на 9 часов парализовать антитеррористический фронт Государственного департамента США (См: http://www.crime-research.ru)

ской помощи, системы управления полетами или системы безопасности[1].

Степень угрозы со стороны кибертерроризма сложно оценить, отчасти потому, что известные и крупные криминальные и террористические организации дополняются большим количеством мелких радикальных групп и террористов-одиночек, а опасность от них, как показывает практика, примерно одинакова. В любом случае возможности хакеров огромны. Правда, степень вероятности совершения терактов в киберпространстве существенно варьируется в различных странах. США и Европа практически уже живут в эпоху кибертерроризма, и угроза эта ими осознана. Россия пока эту угрозу воспринимает лишь как абстрактную, а вместе с тем, на наш взгляд, необходимо глубокое изучение данной темы наряду с осознанием проблемы информационной безопасности и государством, и пользователями всемирной сети.

С учетом растущей в условиях глобализации взаимозависимости экономик и необходимости развития межгосударственного сотрудничества политика в области борьбы киберугорозой нуждается в соответствующей корректировке.

Е.Е. Рыбакова

Кибертерроризм как одна из разновидностей киберпреступности: понятие и виды

Угроза кибертерроризма уже не первое десятилетие достаточно широко (многосторонне) обсуждается в современном обществе на самых разных уровнях, порождая множество научных споров, мифов и спекуляций. Неадекватная оценка рисков, связанных с осуществлением этой угрозы, приводит как к недооценке, так и к переоценке ее серьезности. В результате наряду с «устрашающими» описаниями глобальных катастроф, нередко встречается и полное игнорирование этой проблемы. Например, некоторые представители Европейского Союза и стран Североатлантического Союза обвиняют американское правительство, продавцов информационных технологий, а также средства массовой информации в искусственном создании угрозы кибертерроризма.“Угроза кибертерроризма в значительной степени «раздута»”, - считает Брюс Шнеер, основатель и технический директор Counterpane Internet Security Inc. в Капертино (США, штат Калифорния). “Если я не могу целый день прочитать свою электронную почту, это ещё не означает, что я подвергся кибератаке. От крупномасштабных кибератак, последствия от которых можно будет сравнить со взрывом мощнейшей бомбы,

[1] Подробнее см. Современная проблема международной киберпреступности. // Борьба с преступностью за рубежом. 2001. № 2. Стр. 18 – 19.

нас разделяют десятки лет научно-технического прогресса. Всё это ещё впереди”.[1]

Некоторые отечественные и зарубежные специалисты в области информационных технологий безопасности, защиты программного обеспечения операционных систем также разделяют подобное мнение.

«Кибератака коренным образом отличается от использования террористами Internet-сети как средства коммуникации», - заявил Рейнер Фас (Rainer Fahs), главный инженер по информационной защите при командовании военно-воздушными силами НАТО.[2]

При наличии некоторых существенных разногласий и споров все специалисты из области информационных технологий сходятся в одном:

- элементы критической инфраструктуры пусть косвенно, но зависят от Internet-сети, их безопасность всегда основывалась на защите компьютерной. Подключение к сети Интернет открывает дополнительные возможности проникновения злоумышленников в компьютерные системы, однако, сам факт наличия такого подключения не следует во всех случаях рассматривать как уязвимость. Серьезные меры по резервированию данных и оборудования, предпринимаемые предприятиями различных отраслей, в большинстве случаев обеспечивают адекватный уровень защищенности, даже в случае успешного осуществления кибератаки сети;

- угрозу кибервойны не стоит преувеличивать, но нельзя и недооценивать. Кибератаки действительно могут иметь серьезные последствия, хотя и не связанные с нанесением ущерба жизни и здоровью людей, массовыми разрушениями и другими катастрофами. В наихудшем сценарии, хорошо спланированная массированная кибератака может временно вывести из строя системы телекоммуникаций в густо населенных районах.

Прежде чем перейти к анализу сложного феномена кибертерроризма, необходимо определиться с более общим понятием «киберпреступности». Термин «киберпреступность» российскими и международными нормативными правовыми актами официально не зафиксирован. Каждая организация, государство и авторы любого закона располагают собственным мнением о том, что является киберпреступлением и киберпреступностью, а что нет. Многочисленные попытки создания пригодной дефиниции киберпреступности и связанных с ней терминов иллюстрируют, что это такой широкий и обобщенный термин, что эти попытки практически бесполезны. *В данном случае необходимо разработать типовое определение киберпреступности*. Важность единой терминологии заключается в

[1] Не преувеличена ли угроза кибертерроризма? www.crime-research.org
[2] Не преувеличена ли угроза кибертерроризма? www.crime-research.org

том, что если мы не будем использовать одинаковые – или, по крайней мере, существенно не отличающиеся – определения, единый подход к киберпреступлениям будет невозможен. Невозможен будет также сбор достоверных статистических данных, предназначенных для правового анализа способов совершения киберпреступлений и тенденций развития и трансформации киберпреступности.

В соответствии с рекомендациями экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети[1]. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде. Преступление, совершенное в киберпространстве это виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ. Подчеркну, что понятие киберпреступность не ограничивается рамками преступлений, совершенных в глобальной информационной сети Интернет, она распространяется на все виды преступлений совершенных в информационно-телекоммуникационной сфере, где информация, информационные ресурсы, информационная техника могут выступать (являться) предметом (целью) преступных посягательств, средой, в которой совершаются правонарушения, и средством или орудием преступления.

Одна из наиболее опасных разновидностей киберпреступности ― кибертерроризм также требует корректного определения. Переход в промышленности и иных сферах деятельности на методы электронного управления технологическими процессами послужил основанием для появления нового вида терроризма – кибертерроризма, который проявляется во вмешательстве в работу компонентов телекоммуникационных сетей, функционирующих в их среде компьютерных программ, несанкционированной модификации компьютерных данных, что вызывает дезорганизацию работы критически важных элементов инфраструктуры государства и создает опасность гибели людей, значительного имущественного ущерба или иных общественно опасных последствий.

Кибертерроризм представляет собой серьезную социально опасную угрозу для человечества, причем степень этой угрозы в силу своей новизны, обществом не до конца еще осознана и изучена. Опыт, который уже имеется у мирового сообщества в этой области,

[1] См.: Преступления, связанные с использованием компьютерной сети / Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями //A/CONF. 187/10.

со всей очевидностью свидетельствует о несомненной уязвимости любого государства, тем более что кибертерроризм не имеет государственных границ, кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара.

К сожалению, многие средства массовой информации употребляют термин «кибертерроризм» весьма некорректно, создавая путаницу в понятиях, ставя знак равенства между понятием «хакер» и «кибертеррорист». Вряд ли это можно счесть правильным. Безусловно, терроризм - это преступление, но не каждое преступление есть терроризм, точно так же как кибертеррориста, как правило, можно назвать хакером, но не всякий хакер совершает терракты в киберпространстве или с помощью компьютера. Именно корректное определение того или иного явления позволяет увидеть его суть, и, если это явление имеет негативные последствия, то выявить формы и методы борьбы с ним. Итак, на наш взгляд, кибертерроризм можно отнести к так называемым технологическим видам терроризма. В отличие от традиционного, этот вид терроризма использует в террористических акциях новейшие достижения науки и техники в области компьютерных и информационных технологий, радиоэлектроники, генной инженерии, иммунологии. Сам термин «кибертерроризм» появился в IT-лексиконе предположительно в 1997 году. Именно тогда специальный агент ФБР Марк Поллитт определил этот вид терроризма как «преднамеренные политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов».[1]

Известный эксперт в области обеспечения безопасности информационных технологий Д. Деннинг говорит о кибертерроризме как о «противоправной атаке или угрозе атаки на компьютеры, сети или информацию, находящуюся в них, совершенную с целью принудить органы власти к содействию в достижении политических или социальных целей».[2]

Исследователи М. Дж. Девост, Б. Х. Хьютон, Н. А. Поллард определяют информационный терроризм (а кибертерроризм является его разновидностью) как:

(1) соединение преступного использования информационных систем с помощью мошенничества или злоупотреблений с физическим насилием, свойственным терроризму;

(2) сознательное злоупотребление цифровыми информационными системами, сетями или компонентами этих систем или сетей

[1] См. Krasavin S. What is Cyber-terrorism? // http://iTjai§.org/mfowar.
[2] Denning D. E. " Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" http://www.nautilus.org/info-policy/workshop/denning.html.

в целях, которые способствуют осуществлению террористических операций или актов".[1]

Кибертерроризм использует открытость Интернета для дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния, что порождает страх и тревогу, и является своего рода дополнением к традиционному виду терроризма.

По мнению, Тропиной, можно выделить два вида кибертерроризма: совершение с помощью компьютеров и компьютерных сетей террористических действий (условно назовем это терроризмом в «чистом виде»), а также использование киберпространства в целях террористических групп, но не для непосредственного совершения терактов.

Первому виду кибертерроризма можно дать определение с помощью соединения двух понятий «киберпространство» и «терроризм». Терроризм (в соответствии со статьей 205 УК РФ) есть совершение взрыва, поджога или иных действий, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если эти действия совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза совершения указанных действий в тех же целях. Таким образом, кибертерроризм «в чистом виде» есть умышленная атака на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающая опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. Это деяние должно быть совершено в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти. К этому виду терроризма можно отнести также угрозу совершения подобных действий для достижения вышеуказанных целей.[2]

Второй вид кибертерроризма, подразумевает использование киберпространства террористическими группами для осуществления и популяризации своей деятельности, но не для непосредственного совершения терактов, а для имущественного, финансового и информационного обеспечения террористической деятельности. Сюда

---

[1] Цит. По Томас Тимоти Л. Сдерживание ассиметрических угроз, стоящих перед обществом в информационную эпоху.//Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции.М.,2002.-С.165.

[2] Тропина Т.Л., исследователь Владивостокского Центра по изучению организованной преступности. Киберпреступность и кибертерроризм. //www.crime-research.org

входят связь друг с другом, планирование, изыскание денег, сбор разведывательной информации, вербовка и распространение информационно-пропагандистских материалов.

Террористические акции в киберпространстве могут совершаться не только отдельными лицами или террористическими группами, но и одним государством против другого. В этом кибертерроризм ничем не отличается от любого другого вида терроризма. Экстремистские группировки, сепаратистские силы, проповедники идей, противоречащих общечеловеческим ценностям, интенсивно используют современные технологии для пропаганды своей идеологии и ведения информационных войн.

С учетом большого количества мотивов совершения актов кибертерроризма можно предположить, что в ближайшее время произойдет еще большая криминологическая, правовая и информационная классификация кибертерроризма как разновидности киберпреступности и увеличится количество научных исследований, посвященных данной проблематике. Поэтому исследования проблем противодействию кибертерроризму еще длительное время актуальными и практически значимыми.

Джеймс А. Льюис

Оценка риска кибертерроризма, кибервойны и других киберугроз[1]

Слово «кибервойна» ассоциируется с образами неких таинственных бойцов, атакующих в киберпространстве компьютерные сети и ничего не подозревающего противника, при этом наносящих ущерб и парализующих деятельность человечества. Так какова же вероятность того, что этот устрашающий сценарий станет явью? Каковы были бы результаты нападений в киберпространстве, произойди эти нападения в реальности?

Кибератаки, безопасность сетей и информации – это сложные проблемы, представляющие собой новую область для исследований

---

[1] James A. Lewis. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats Center for Strategic and International Studies. Washington, D. C. December 2002. Перевод Т.Л. Тропиной.

[1] U.S. Strategic Bombing Survey, Summary Report (European War), 1945.// http://www.anesi.com/ussbs02.htm

в сфере национальной безопасности и политики. Эта статья посвящена только одному аспекту проблемы: вопросам кибертерроризма и атак на важные инфраструктуры, а также национальной безопасности в этой сфере. Кибертерроризм – это «использование компьютерных сетей в качестве средства для нарушения функционирования важнейших национальных инфраструктур (энергетических, транспортных, правительственных) или понуждения или запугивания правительства или гражданского населения». Предпосылкой кибертерроризма является то, что функционирование человека и работа важнейших инфраструктур стали все больше зависеть от компьютерных сетей. Таким образом, появилось уязвимое место, «огромная электронная Ахиллесова пята». Враждебная нация или группа могут использовать эту уязвимость для проникновения в плохо защищенную компьютерную сеть и нарушения работы важнейших инфраструктур, вплоть до полной остановки их функционирования.

Большая часть литературы о кибертерроризме предполагает, что компьютерные сети уязвимы так же, как важнейшие структуры обеспечения деятельности человека, и эта уязвимость подвергает огромному риску национальную безопасность. Учитывая новизну компьютерных технологий и скорость, с которой они проникают в экономическую деятельность, эти предположения закономерны. Но более пристальное рассмотрение взаимосвязи компьютерных сетей и важнейших инфраструктур, их уязвимости к атакам и значения нападений для национальной безопасности, приводит к выводу, что первоначальные данные об уязвимости не совсем верны. В данной статье мы не сможем дать полную переоценку, поскольку ограничены рамками статьи, но уже краткий обзор показывает, что в то время как множество компьютерных сетей остаются очень уязвимыми для нападений, не все важнейшие инфраструктуры настолько уязвимы.

Переоценка киберугрозы имеет четыре составляющие. Сначала необходимо провести анализ кибервойны и кибертерроризма в историческом контексте – т. е. в истории нападений на инфраструктуру. Стратегии, акцентирующиеся на нападениях на важнейшие инфраструктуры, обсуждаются уже более 80 лет.

Во-вторых, мы должны проанализировать кибератаки на фоне обычных аварий, происходящих в этой сфере. Ведь есть статистические данные об отключениях электричества, задержках полетов, авариях на коммуникациях, которые случаются и в нормальной обстановке, и последствия этих аварий и сбоев могут служить индикатором для определения возможных последствий кибертерроризма и кибервойны.

В-третьих, мы должны определить степень зависимости инфраструктуры от компьютерных сетей, а также определить избыточ-

ную зависимость, уже представленную в некоторых системах. Наконец, в случае с кибертерроризмом, мы должны рассмотреть возможность использования кибероружия в политических целях и в качестве средства для террористов, а также вероятность достижения этих целей с помощью кибероружия.

Предварительный обзор данных факторов показывает, что уязвимость компьютерных сетей становится все более серьезной проблемой для бизнеса, но угроза для национальной безопасности все-таки преувеличена. Современное индустриальное общество является более устойчивым, чем представляется на первый взгляд. Важнейшие системы обеспечения в больших экономических системах при рыночной экономике более распределены, разнообразны, избыточны и способны к самовосстановлению, чем может показать поверхностная оценка, что делает их менее уязвимыми к нападениям. Во всех случаях, кибератаки менее эффективны и разрушительны, чем физические нападения. Их единственное преимущество состоит в том, что они значительно дешевле и более легки по исполнению, чем атаки физические.

Инфраструктура как мишень

Кибертерроризм – не первый случай, когда новую технологию взяли на вооружение для создания стратегической уязвимости. Конечно, нельзя сказать о том, что теории кибервойны и войны авиационной идентичны, но сравнить их полезно. После Первой мировой войны, учтя ее опыт, европейские стратеги, такие как Доухет и Тренчард, утверждали, что воздушные бомбардировки далеко от линии фронта в тылу противника нанесут непоправимый вред его способности вести войну. Их теории были взяты на вооружение и испытаны Армией США и Королевскими воздушными силами во время Второй мировой войны в кампаниях стратегических бомбардировок, нацеленных на разрушение электрических и транспортных сетей, производственных мощностей. Большая часть первых трудов, посвященных кибератакам, напоминает во многом (и многим обязана) ранней литературе о стратегических бомбардировках.

Важнейшим документом для понимания того, какой вред атаки на инфраструктуру наносят обществу, является «Обзор стратегических бомбардировок», данные для которого собраны США во время и после Второй мировой войны. Во время войны Великобритания и США, стремясь уничтожить индустриальную базу противника и отбить у населения желание продолжать войну, выпустили тысячи тяжелых бомбардировщиков, которые сбросили на Германию миллионы тонн взрывчатых веществ. Ранние теоретики воздушной войны предсказывали, что подобные нападения парализу-

ют противника или нанесут ему вред. Однако обзор показывает, что индустриальные общества весьма эластичны. Промышленность в течение двух лет бомбежек только увеличивала свои показатели, а сопротивление прекратилось только после того, как Германию заняли сухопутные войска.

Поскольку воздушное наступление наращивало темпы, немцы не могли предотвратить вред, нанесенных их экономике и, в конечном счете, ее крах. Однако восстановительные и защитные способности Германии были огромны, скорость и изобретательность, с которыми эта страна восстанавливала и поддерживала производительность основных отраслей промышленности и проведение военных операций, явно превзошли все ожидания союзников. Германия использовала все мыслимые средства, которые только можно было изобрести, чтобы избежать атак на свою экономику или нейтрализовать их эффекты.

Существенна и психическая реакция немецкого народа на воздушные нападения. Под безжалостным нацистским режимом, народ показал ошеломляющее сопротивление ужасу непрекращающихся воздушных атак и сопряженным с ними трудностям, разрушению домов и имущества, обстоятельствам, в которых было очень сложно выжить. Их моральный дух, их вера в окончательную победу или в устраивающий всех компромисс, а также вера в лидеров снижались, но они продолжали эффективно работать, пока оставались физические средства производства[1].

США определили, что те же самые результаты воздушных бомбардировок показала Вьетнамская война. В разрез с логикой, эффектом воздушных атак было укрепление длительного сопротивления и рост количества тех, кто его поддерживал. Появление ядерного оружие (и боеприпасов, наводящихся с большой точностью) дало авиации возможность большего разрушения гражданских инфраструктур, и должно было, наконец, достигнуть целей, указанных Доухетом, Тренчардом или Митчеллом, но кибератаки не могут повлечь за собой такой же уровень летальных исходов.

Один из выводов «Обзора стратегических бомбардировок» заключается в том, что «немецкий опыт показал, что, безотносительно системы целей, никакая необходимая промышленность не выводилась из строя одной атакой. Необходимы были постоянные атаки». Однако кибератаки по всей вероятности должны происходить в виде отдельных нападений. Как только хакер получил доступ и нанес ущерб, адресат обычно быстро реагирует и пытается закрыть брешь, позволившую осуществить атаку, и привести системы в рабочее состояние. В кибератаках злоумышленники должны были

[1] «Weapons of mass annoyance» - «Оружие массового раздражения»: выражение принадлежит Стюарту Бэйкеру (Stewart Baker).

бы непрерывно находить новые бреши и изобретать новые тактики, чтобы гарантировать длительный сбой. Кибератаки редко наносят физический ущерб, требующий длительного ремонта.

Стандартные сбои vs. кибератаки.

Защита важнейших инфраструктур создает новые проблемы для национальной безопасности. Здесь вовлечено множество действующих лиц. В фокусе – гражданские и коммерческие системы и услуги. Военная сила менее важна. Размах этих новых проблем зависит от того, как мы определяем национальную безопасность, и какой порог допустимого ущерба нами установлен. В перспективе общественной безопасности, ни одна страна не хочет допустить даже одного нападения на инфраструктуры или системы оказания услуг. Если цель состоит в том, чтобы воспрепятствовать кибератаке, которая будет равна по стоимости, например, одному дню водоснабжения или обеспечения населения электроэнергией, мы установим очень высокий стандарт защиты. Однако, в стратегической военной перспективе, нападения, которые не ухудшают национальные возможности, несущественны. В этом контексте, если кибератака не причиняет убытки, которые превышают порог стандартных сбоев, нормальных для каждой экономики, это не является непосредственных и существенным риском для национальной безопасности.

Особенно важно отметить, что в контексте макроэкономики сбои в системах водоснабжения, перебои с электроэнергией, сбои воздушного движения и другие «сценарии» кибртеррора – стандартные события, которые не затрагивают национальную безопасность. Для национальной экономики, где десятки или даже сотни систем обеспечивают важнейшие инфраструктуры, сбой в системах, когда обслуживание потребителей прекращается на часы или дни – стандартный случай на региональном уровне. Кибертеррористы должны атаковать множество целей одновременно и продолжать атаку в течение довольно долгого периода, для того, чтобы посеять ужас и достигнуть стратегических целей, или даже любого значимого эффекта. Относительно большинства важнейших инфраструктур, такой сценарий множественных нападений неосуществим для хакеров, террористических групп или государств (особенно для государств, когда риск разоблачения, и рассмотрения происходящего как акта военной агрессии превосходит ограниченные преимущества, которые можно получить от кибернападений на инфраструктуру).

Оружие массового раздражения [1]

[1] Barton Gellman, " Cyber attacks by al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool," The Washington Post, June 27, 2002.

Детальная экспертиза некоторых сценариев нападения на важнейшие инфраструктуры помогает более точно определить значение кибератак в стратегическом контексте или в контексте национальной безопасности. Например, дамбы или плотины, используемые для хранения воды и выработки электричества, часто называются в качестве вероятной мишени кибератак. Недавно «Вашингтон Пост» процитировал «пожелавших остаться неизвестными» американских аналитиков, полагающих, что «отключив или взяв под контроль команды шлюзов дамб или подстанций, вырабатывающих до 300 000 вольт электроэнергии, злоумышленник может при помощи виртуальных средств уничтожить реальную собственность и жизни людей» [1].

В США системы водоснабжения недосягаемы для кибератак. Соединенные штаты имеют 54 064 сепаратных систем водоснабжения. Из них 3769 систем обслуживают 81% населения, и 353 системы – 44% населения. Однако такое неравномерное распределение только усложняет задачу террористов. Многие из этих систем водоснабжения, даже те, что находятся в больших городах, продолжают использовать технологии, которые нелегко разрушить сетевыми нападениями. В США были случаи, когда водоснабжение было нарушено на протяжении многих дней (обычно в результате наводнения), но эти случаи не имели эффекта ужаса и не парализовали никого и ничего. Кибертеррористы или кибервоины должны осуществить длительную атаку, которая одновременно разрушит несколько сотен из этих систем, чтобы получить какую-либо стратегическую выгоду.

Мы можем предположить, что если террорист найдет уязвимость в системе водоснабжения, которая позволит оставить на какой-то период без воды некий населенный пункт, то эта брешь может быть использована для увеличения ущерба от физического нападения (например, в случае пожара не будет воды для тушения). Вообще, последствия кибернападения, которое может пройти незамеченным в «нормальном беспорядке» ежедневной жизни, могут многократно возрасти, если оно будет сочетаться с физическим нападением. Одновременное использование физического нападения и кибератак – единственный способ сделать кибероружие привлекательным для террористов. Американская ассоциация работников водоснабжения наиболее вероятным источником террористической

[1] DeNileon, Guy, “The Who, What Why and How of Counter-terrorism Issues,” American Water Works Association Journal, May 2001, Volume 93, No. 5, pp. 78–85, http://www.awwa.org/Communications/journal/Archives/J501es3.htm, see also Scott Berinato, “Debunking the Threat to Water Utilities,” CIO Magazine, March 15, 2002, http://www.cio.com/archive/031502/truth_sidebar2.html

угрозы системам водоснабжения называет именно «физическое разрушение компонентов системы поставки воды» [1].

Сравнение авиационных атак и кибернападений на гидроэлектрические сооружения помогает определить степень киберугрозы. В начале Второй мировой войны Королевские воздушные силы осуществили смелое нападение на дамбу в Руре, главный источник электрической энергии для немецкой промышленности. Нападение имело успех, дамба была разрушена бомбами, и обеспечение региона электричеством на время было прервано[2]. Сопоставимое кибернападение произошло в США, когда молодой хакер получил доступ к компьютерному управлению дамбой на Юго-Западе Соединенных Штатов, но ему не удалось ни прервать производственный процесс, ни причинить физический ущерб[3]. Ни одна из этих атак не парализовала производство электроэнергии. Из двух приведенных примеров, кибератака была менее эффективна, поскольку не причинила физического ущерба и могла быть классифицирована не как угроза, а скорее как «раздражение». Воздушная атака привела к физическому повреждению, которое могло быть восстановлено, и было восстановлено. Единственное преимущество кибератаки – в том, что это менее дорого: подросток и персональный компьютер, а не дорогостоящий самолет с оборудованием и экипажем.

Множество исследований посвящено кибертеррористам, прекращающим работу систем выработки электроэнергии. Один из лучших обзоров, посвященных кибератакам, нашел, что энергетические компании – первая мишень кибератак, и что 70% этих компаний «подверглись серьезному нападению» в течение первых шести месяцев 2002 года[4]. Американские электрические сети – лакомый кусок для террористов, но эти сети являют собой совокупность множественных избыточных систем, в которых неудачи и сбои являются стандартной ситуацией. Национальная электрическая сеть – это взаимоувязанная система, состоящая из более чем 3000 государственных и частных предприятий. Эти 3000 поставщиков электроэнергии используют различные информационные технологии для управления процессом получения и передачи энергии. Хакер или даже большая группа хакеров должна найти бреши во множестве систем, чтобы произвести значительный сбой в энергоснабжении, но даже в этом случае атака может прервать энергообеспечение лишь на несколько часов.

---

[1] The Germans quickly repaired the damage and production in the Ruhr actually increased after the attack. There were a number of civilian casualties, but most of these were Soviet prisoners of war who were trapped in their prison camp and unable to escape the initial flood. Cyber attacks that open floodgates would not produce the same surge of water as an explosive breach.

[2] Lemos, Robert, “Cyber Terrorism, the Real Risks,” ZDNet News UK, August 27, 2002, http://news.zdnet.co.uk/story/0,,t269-s2121358,00.html

[3] Riptech Internet Security Threat Report, July 2002, http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf

Североамериканский Совет надежности электроснабжения, промышленная группа, сформировавшаяся после отключения света в Нью-Йорке в 1965 году, работала с 1980-х годов совместно с Правительством для улучшения электрической системы и выработки способов быстрого восстановления системы после больших сбоев. Из отчета должностных лиц этой организации перед Конгрессом следует, что в последние несколько лет ни вирусы, ни иные компьютерные атаки против американской системы электроснабжения не прервали электроснабжение[1]. И хотя источники в промышленности могут рисовать более оптимистическую картину, факт остается фактом – падающие деревья вызывают множество сбоев в системе электроснабжения, в то время как кибератаки – ни одного. Оценка риска Информационной группой Комиссии по консультациям в области безопасности национальных телекоммуникаций заключает, что «физическое разрушение все еще представляет самую большую угрозу, с которой может столкнуться энергетическая инфраструктура. По сравнению с этим, электронное вторжение представляет собой уже появившуюся, но все еще относительно незначительную опасность» [2].

США уже провели крупномасштабный эксперимент по выходу из строя систем энергоснабжения на опыте Калифорнии, где в прошлом году был отменен государственный контроль в этой сфере. Усилия Калифорнии по прекращению государственного регулирования привели к месяцам простоев и перебоям напряжения в штате. Отмена государственного контроля была более мощным «нападением» на инфраструктуру, чем предполагаемые или уже осуществленные нападения кибертеррористов. Ясно, что Калифорния понесла экономические потери, но это не покалечило государство и не посеяло ужас. Точно так же падения напряжения по всей стране в 1999 году затронули миллионы людей и обошлись энергетическим компаниям в миллионы долларов убытков. Эти сбои были вызваны увеличением потребления электричества в связи с тем, что в течение длительного времени летом держались высокие температуры. В отличие количества сбоев, произошедших в связи с отменой государственного контроля в Калифорнии или жаркой погодой, количество сбоев в США, вызванных хакерами или кибертеррористами, остается нулевым.

Вмешательство в национальные системы управления полетами для того, чтобы прервать связь при осуществлении воздушных рейсов и подвергнуть опасности пассажиров и экипаж, - другая час-

[1] Testimony of Michehl R. Gent Before the Senate Government Affairs Committee, May 8, 2002, ftp://www.nerc.com/pub/sys/all_updl/docs/testimony/mrg-testimony-SenateGovernmentalAffairs-5-08-02-(final).pdf

[2] Information Assurance Task Force of the National Security Telecommunications Advisory Committee http://www.aci.net/kalliste/electric.htm

то упоминаемая киберугроза[1]. Но мы еще не находимся на том уровне, когда самолет дистанционно ведется компьютерными сетями, так что для кибетеррориста невозможно получить полный контроль над самолетом. В самолетах все еще есть пилоты, которые обучены действовать в критических ситуациях. Точно так же Федеральное авиационное агентство (FAA) не зависит исключительно от компьютерных сетей в качестве средства для управления полетами, и при этом связь, которая используется, не зависит от Интернета. Высокая степень вовлеченности человека в управление воздушным транспортом и процессы принятия решений в этой сфере уменьшает риск кибернападения. Ежемесячно происходят штормы, отказывает электричество, случаются сбои в программах, - все это обусловливает высокий уровень сбоев в воздушном движении. Однако пилоты и диспетчеры приучены к неожиданным сбоям, и действуют так, чтобы уменьшить их отрицательный эффект. Авиакомпании и пассажиры также привыкли к высокой степени сбоев в системе, это не является для них неожиданностью. В США нормой является 15000 – 20000 отложенных или отмененных рейсов в месяц. Кибернападение, которое ухудшило бы систему воздушного движения, создаст задержки и вызовет раздражение, но никакого риска для национальной безопасности не представит.

FAA имеет 90 основных компьютерных систем и 9 различных систем коммуникаций. Эти сети полагаются на довольно-таки старое оборудование и используют частное программное обеспечение, что затрудняет их взлом со стороны. Этим объясняется тот факт, что немногие нападения, о которых известно, нарушили воздушное движение. В одном из известных инцидентов, молодой хакер прервал местную телефонную связь в Новой Англии, отрезав от связи контрольно-диспетчерский пункт регионального аэропорта и вызвав сбой в системе включения огней взлетно-посадочной полосы. Хотя сбой продолжался шесть часов, в аэропорту не произошло ни одного несчастного случая. Еще был случай, когда компьютерные сети штаба FAA открылись для хакеров, предоставляя информацию о пассажирах и разрешая считывать действия, а также случай, когда хакеры получили доступ к почте FAA. Ни один из этих случаев не привел к сбою полетов[2]. Как ни странно, модернизация может фак-

[1] Larissa Paul, “When Cyber Hacktivism Meets Cyberterrorism,” SANS Institute, February 19, 2001 “Examples of cyber terrorist actions can include hacking into an air traffic control system that results in planes colliding….»

[2] Sascha Segan, “Safety At Risk, “ ABC News.com, September 27, 2000, http://abcnews.go.com/sections/tech/DailyNews/gao_faa000927.html, General Accounting Office, “Air Traffic Control: Weak Security Computer Practices Jeopardize Flight Safety,” GAO-AIMD 98-155, http://www.gao.gov/archive/1998/ai98155.pdf

[2] Keith Bradsher, “With Its E-Mail Infected, Ford Scrambled and Caught Up,” The New York Times, May 8, 2000

тически увеличить уязвимость FAA, если наибольшее внимание при этом не уделять защите.

Недавние Интернет-атаки иллюстрируют природу уязвимости киберпространства к атакам. В октябре 2002 года в течение часа неизвестные злоумышленники произвели атаку на 13 корневых серверов, которые формируют систему доменных имен, управляющую адресами Интернет. Восемь из тринадцати серверов из-за атаки были недоступны. Сама атака прошла практически незамеченной и не оказала никакого действия на пользователей Интернет. Нападение на систему доменных имен заметно не ухудшило работу Интернет. Большинство данных системы доменных имен, необходимых для выполнения ежедневных операций, сохранено локально и ежедневно модифицируется. Очень немногие запросы требуют помощи корневых серверов. Кроме того, присутствие тринадцати серверов (из которых пять нападением не были затронуты) является некоторым избытком, который предполагает, что если в Интернет есть брешь, то серверы системы доменных имен таковой не являются. Вскоре после того, как произошли атаки на систему доменных имен, тысячи пользователей Интернет на Западе США испытали серьезные задержки работы сети, когда в у их провайдера начались проблемы с маршрутизацией из-за программных ошибок. В отличие от атак со стороны, этот сбой фактически нарушил работу, но также не имел никакого эффекта для национальной безопасности.

Хотя Интернет может иметь несколько точек, сбой в которых приведет к сбою всей системы, изначально данная сеть была разработана в качестве устойчивой системы коммуникации, способной к продолжению операций даже после ядерного удара. Пакетная коммутация и Интернет-протоколы были разработаны для того, чтобы связь не прерывалась даже в случае повреждения некоторых узлов сети, и сам Интернет был предназначен для того, чтобы обойти повреждение и позволить связи продолжаться, не прерываясь. Кроме того, компьютерные сети основываются на сетях передачи данных большой емкости, относительно защищенных от кибератак. Введение новых технологий связи также увеличивает жизнеспособность Интернет. Беспроводная и спутниковая связь создает даже некоторый избыток систем наземных линий связи. Большинство индустриальных стран теперь имеет доступ к трем или четырем различным режимам связи, что делает систему значительно более устойчивой, чем десятилетие назад. Увеличение использования ультра широкополосных и радио сетей также создает избыточность сетей и увеличивает жизнеспособность систем коммуникаций против кибератак.

Служба помощи в чрезвычайных ситуациях 911 – специализированная коммуникационная система, которая основывается на

местной телефонной сети, является в представлении теоретиков также одной из самых привлекательных целей, но, как и другие важнейшие инфраструктуры, эта мишень очень устойчива. Например, США используют не одну систему 911, а несколько тысяч локальных систем, использующих различные технологии и процедуры. Ни одна система 911 в крупном городе не была взломана. Можно послать множество сообщений по электронной почте с просьбой срочно связаться со службой 911 для получения важной информации, чем перегрузить систему (как это произошло в США в 1997 году). Эта методика может сработать только один раз, но в сочетании с бомбежками или иными физическими нападениями она действенна, поскольку в несколько раз усиливает их эффективность действий террористов.

Производство и экономическая деятельность все больше и больше зависят от компьютерных сетей, киберпреступления и индустриальный шпионаж – новая опасность для экономической деятельности. Однако доказательства уязвимости производства к кибератакам весьма противоречивы. Так, в 2000 году вирус поразил 1000 компьютеров в компании «Форд Мотор». Перед тем, как сеть прекратила работу, компания получила 140000 зараженных вирусом почтовых сообщений. В течение недели в компании не работала почтовая служба. Однако компания сообщила, что «программа злоумышленников, похоже, причинила весьма ограниченный ущерб. Ни одна из 114 фабрик не остановилась. Компьютеризованные технические проекты и другие технические данные остались незатронутыми, компания имела возможность отправлять информацию дилерам и поставщикам автомобилей через специальные сайты»[1]. Сейчас компания сообщает, что предпринятые ими меры защиты превращают вирусы, которые были весьма разрушительными, когда появились впервые, в мелкие неприятности[2].

Кибератаки часто представляются как угроза военным силам, и сети Интернет отводится большая роль в войне и шпионаже. Информационная война подразумевает целый диапазон действий, в ряду которых кибератаки играют далеко не самую важную роль. В то время как информационные операции и информационное превосходство стали важными элементами для проведения успешных военных операций, ни одна нация не поставила свои военные силы в такое положение, когда они зависели бы от компьютерных сетей, которые очень уязвимы к внешнему нападению. Это существенно ограничивает эффективность кибероружия (код, посланный по компьютерным сетям). Множество поступающих сообщений о

---

[1][32] Riptech Internet Security Threat Report, July 2002.

[2][33] Buchan, Glenn C., "Implications of Information Vulnerabilities for Military Operations," in Khalilzad and White, The Changing Role of Information in Warfare, Rand, 1999

взломе военных компьютерных сетей, обычно не содержат информации о том, используются ли эти сети для важных военных функций. Однако показательно то, что, несмотря на регулярные сообщения о десятках тысяч ежегодных нападений на сети Министерства обороны, не произошло никакой деградации военных возможностей США.

Например, во время операций в Косове военные компьютерные сети США подверглись множеству нападений, но эти нападения не привели к отмене военных операций или потерям. Точно так же вряд ли преуспеет иностранное государство, пожелай оно использовать кибероружие для предотвращения выступления авианосца с боевыми силами на борту. Недавнее нападение британского хакера не поставило под угрозу ни информационные ресурсы, ни военные операции. Исследование Рэнда об информационной уязвимости воздушных сил США при проведении военных операций говорит, что:

«в то время как большинство текущих актуальных интересов сосредоточилось на более новых, модных угрозах информационным системам, особенно взломах компьютеров и связанные с этим сбои и манипуляции … наш анализ показал, что некоторые из «старомодных» угроз представляют большую опасность.» [1]

Хакерство и терроризм

Большая часть ранних работ о «киберугрозе» изображает хакеров, террористов, иностранных шпионов и преступные группировки, которые, вбив в компьютер несколько команд, могут получить контроль над важнейшими инфраструктурами или разрушить их, а также парализовать целые нации. Этот пугающий сценарий не подкрепляется никакими доказательствами. Террористические группы, подобные Аль Каеде, действительно широко используют Интернет, но только как средство связи внутри группы, сбора средств и популяризации своей деятельности. Кибертеррорист может также использовать Интернет в своих целях, чтобы узнать номера кредитных карт или иные ценные данные, необходимые для обеспечения финансовой поддержки террористических операций. Кибертерроризм привлекает значительное внимание, но до настоящего времени он являлся не многим больше, чем пропаганда, некая совокупность сведений или цифровой эквивалент надписей на стенах, с группами, стирающими сайты друг друга. Никакие важнейшие инфраструктуры не пострадали от кибератак.

Террористы стремятся сделать политические заявления и причинить психологический и физический вред объектам своих атак. Если терроризм представляет собой насильственное действие, направленное на достижение политических целей, насколько по-

[1] This is not an argument for self-censorship, as the economic and political benefits of openness and

лезным террористы находят экономическое оружие, которое достигает эффекта не сразу и в совокупности с другими средствами? Одно из руководств по обучению, которое используется в Аль Каеде, «Военные учения в джихаде против тиранов», обращает внимание на то, что взрывчатые вещества – наиболее предпочтительное оружие террориста потому что «взрывчатые вещества вызывают у врага с явный ужас и испуг». Взрывы выглядят драматично, вселяют страх в сердца противника и причиняют длительный ущерб. Кибератаки не могут дать того драматического и политического эффекта, которого террористы стремятся достигнуть. Нападение в киберпространстве, которое может пройти даже незамеченным для его жертв, или приписано стандартным задержкам или выходам из строя, не будет для них предпочтительным оружием. Если терроризм есть насильственные действия, которые должны причинить удар и достигнуть политических целей, как террористам могут быть полезны экономические способы ведения войны, эффекты которых являются в лучшем случае постепенными и проявляются в совокупности с другими?

Анализ риска кибертерроризма также усложняется тенденцией изначально приписывать действия в киберпространстве военным или террористам, когда фактически они совершаются гражданскими лицами – развлекающимися хакерами. Когда в конце 1990-ых годов было совершено нападение через сети DOD, первые подозрения США пали на потенциальных противников, в частности, Ирак или Китай. Американские должностные лица обсуждали достоинства активной защиты, а также то, была ли эта атака военным действием, необходимо ли адекватное контрнаступление. После того, как обстановка накалилась, США обнаружили, что атаку организовали два студента средней школы в Южной Калифорнии. Очень трудно, особенно на первых порах или в начале инцидента, определить, кем является напавший: террористом-одиночкой или группой, иностранным государством, преступником, или подростком из Калифорнии. Однако быстрый обзор инцидентов, произошедших за последние четыре года, позволяет предположить, что преступники и скучающие подростки - наиболее вероятные источники нападения. На сегодняшний день, подавляющее большинство инцидентов взломов – действия развлекающихся хакеров.

Хотя СМИ сообщают, что должностные лица в Правительстве обеспокоены планами Аль Каеды по использованию Интернет для кибертеррористических действий, эти истории часто повторяют те гипотетические сценарии, ранее приписываемые усилиям иностранных государств по ведению кибервойны. Риск остается гипотетическим, но врагом теперь выступают не враждебные государства, а группы, подобные Аль Каеде. Единственный элемент новизны, приписываемый Аль Каеде – то, что эта группа могла бы ис-

пользовать кибератаки для закрепления и умножения эффекта от физических нападений. Если кибератаки были бы выполнимы, самый большой риск для национальной безопасности они могут представить только в совокупности с более традиционными методами нападений.

Возможности шпионажа, возникшие в связи с доступностью данных в компьютерных сетях, создадут больший риск для национальной безопасности, чем кибератаки. Террористические группы, вероятно, будут использовать Интернет для сбора информации о потенциальных целях. Разведывательные службы могут не только извлечь выгоду из информации, находящейся в открытом доступе в Интернете, но, [1] что еще более важно, использовать в своих целях возможность тайно проникнуть через компьютерные сети и собрать информацию, которая не доступна публично. Это очень отличается от взлома, потому что в случае успешного проникновения во враждебную сеть, террористическая группа или разведывательная служба будет вести себя настолько скромно и тихо, насколько возможно. Опытный противник может взломать систему и находиться там, собирая сведения и работая, оставаясь незамеченным. Он не будет создавать сбоев в работе или процессе оказания услуг, не будет оставлять тревожные сообщения на сайтах, спокойно собирая информацию «в тени». Методы сбора информации в сети Интернет значительно отличаются от более ранних методов перехвата, и если будут собраны различные виды данных, то это сделает шпионаж более продуктивным. Тема использования компьютерных сетей в качестве средства для шпионажа, заслуживает дальнейшего изучения.

Киберпреступления и экономика.

Кибератаки действительно представляют собой весьма реальный риск, поскольку сети уязвимы перед преступниками, а также велика вероятность того, что экономический ущерб превзойдет во много раз стоимость атаки. Ураган Эндрю, самое дорогое «естественное» бедствие в американской истории, причинил ущерб, который оценивается в 25 миллиардов долларов. Ежегодно средний ущерб от торнадо, ураганов, и наводнений в США оценивается в 11 миллиардов долларов. Напротив, вирус Love Bug, причинил пользователям Интернет, ущерб на сумму от 3 до 15 миллиардов долларов (по различным оценкам). Не будем обсуждать вопрос о том, каким образом подсчитывался этот ущерб (возможно, эти оценки

---

having information available to the public outweigh in almost all cases the potential costs of espionage.

[1] [1] "Extreme Weather Sourcebook," http://sciencepolicy.colorado.edu/sourcebook/composite.html, Richard Wray, "Comptroller estimates city's overall bill at up to $95bn," The Guardian, September 5, 2002. http://www.guardian.co.uk/september11/story/0,11209,786326,00.html, To help put these losses in the context of a $10 trillion national economy, note that the U.S. spent $7 billion in 2002 on Halloween candy.

завышены), но способность одного филиппинского студента университета причинить такой ущерб при помощи недорогого оборудования иллюстрирует потенциальный риск, который представляют киберпреступления для глобальной экономики[1].

Финансовый ущерб от киберпреступлений включает в себя стоимость интеллектуальной собственности, ущерба, нанесенного репутации, а также потери производительности, стоимость обязательств перед третьими лицами. Упущенная выгода (несостоявшиеся сделки, убытки вследствие снижения производительности и т.п.) составляет большую часть убытков, которые причиняются в результате кибератак и вирусов. Однако упущенная выгода не переходит непосредственно в убытки для народного хозяйства. Например, если кибератака, приводящая к отказу сервера в обслуживании, мешает клиентам зайти на сайт продавца книг, они могут обратиться к другому продавцу с той же целью. Совокупная продажа книг на национальном уровне останется прежней, хотя рыночные показатели первого продавца снизятся. Некоторое количество клиентов не пойдет на другой сайт, если первый недоступен, и потери продаж могут возместиться более поздними обращениями клиентов к сайту. Предприниматели терпят большие убытки от финансового мошенничества и воровства интеллектуальной собственности в Интернет, преступлений, количество которых продолжает расти[2].

Отметим еще раз, что проблема защиты киберпространства имеет межнациональный характер. Последние несколько лет ознаменовались появлением опытных преступных группировок, эксплуатирующих бреши в деловых сетях. Их цель - не террор, но мошенничество или сбор экономически ценной информации. Согласно обзорам, посвященным большим корпорациям и компьютерной преступности, воровство коммерческой тайны остается источником самых серьезных потерь[3]. Эти преступления необходимо отличать от вирусных атак и атак посредством отказа в обслуживании. Отказы в обслуживании или вирусы, несут потенциальный вред деловым операциям, но не несут такую же степень риска.

Киберпреступления – серьезная и растущая угроза, но для применения любой страной кибероружия против потенциального противника слишком велик риск для нападающего государства.

---

[1] See: American Society for Industrial Security and PriceWaterhouse-Coopers, 10 th Annual Survey “Trends in Proprietary Information Loss,” http://www.pwcglobal.com/extweb/ncsurvres.nsf/0cc1191c627d157d8525650600609c03/36951f0f6e3c1f9e852567fd006348c5/$FILE/ASIS.pdf, and Computer Security Institute, “2002 Computer Crime and Security Survey,” http://www.gocsi.com/press/20020407.html

[3] http://www.gocsi.com/press/20020407.html

Например, авторы статей в некоторых китайских военных журналах размышляли о том, что кибератаки могли бы вывести из строя американские финансовые рынки. Но дилемма в том, что Китай настолько же зависит от этих финансовых рынков, насколько и США, и от сбоя может пострадать даже больше. Что же касается других важнейших инфраструктур, то размер ущерба, который возможно причинить посредством кибератак, со стратегической точки зрения – тривиален, в то время как потери в случае разоблачения для государств могут быть намного выше. Это утверждение, однако, не распространяется на субъектов, не являющихся государствами, подобно Аль Каеде. Для этих субъектов кибератаки потенциально могут быть полезным средством (хотя и не фатальным и не определяющим).

Заключение

Интернет – новое явление, а новые явления могут представляться более пугающими, чем они есть в действительности. Большая часть ранних работ по анализу киберугроз и киберзащиты написана в стиле «небо падает». Небо не падает, и кибероружие имеет ограниченные возможности для нападения на нацию или запугивания граждан. Примеры, представленные в этой статье, доказывают, что нации более устойчивы и эластичны, чем это представляли ранние теории о кибертерроризме. Для исследования уязвимости важнейших инфраструктур к кибератакам, необходима намного более детальная оценка для каждой инфраструктуры - предполагаемой цели: оценка избыточности инфраструктуры, норм сбоев, степени человеческого участия в управлении, контроле и вмешательство человека в критических ситуациях. Начальная оценка предполагает, что инфраструктуры в больших индустриальных странах устойчивы к кибератакам[1].

Террористы или иностранные вооруженные силы вполне могут начать кибератаки, но эффект, вероятно, их разочарует. Нации более устойчивы, чем предполагают ранние аналитики кибертерроризма и кибервойны, и кибератаки менее разрушительны, чем физические нападения. Цифровой Перл-Харбор маловероятен. Системы инфраструктуры, в силу того, что они постоянно сталкиваются со сбоями, являются более гибкими, способными восстанавливаться, чем полагали ранние аналитики. Кибератака, если она не сопровождается одновременным физическим нападением, которое причиняет физический ущерб, не будет долгой и эффективной. Однако если риск кибертерроризма и кибервойны завышен, риск шпионажа и киберпреступности, возможно, не до конца оценен многими исследователями.

---

[1] I am grateful to Antoin O Lachnain and Michael Yap for pointing out that small countries like Singapore, that do not have the same degree of redundancy, may be more vulnerable.

[1] See Computer Science and Telecommunications Board, National Research Council, Embedded,

Ситуация не статична, и уязвимость важнейших инфраструктур к кибератакам может измениться под воздействием некоторых факторов. Во-первых, она может увеличиться, поскольку общество движется к глобальной вычислительной среде [1], когда привычные действия становятся автоматизированными и все больше зависят от удаленных компьютерных сетей. Во-вторых, уязвимость может увеличиться по мере применения в промышленности и инфраструктуре, особенно использующих диспетчерское управление и сбор данных системы SCADA, новых технологий и движения от частных сетей к связи через Интернет и использования Интернет-протоколов для операций. Это движение можно предсказать с большой уверенностью, учитывая такое преимущество, как стоимость связи через протоколы TCP/IP, а также новые возможности доступа, которые при этом возникают. Эти перемены приведут к увеличению уязвимости, если страны не сбалансируют движение к большей взаимосвязанности сетей и зависимости от связи через Интернет-протокол с усилиями по улучшению сетевой защиты, выработке эффективного механизма юридического принуждения, обеспечению устойчивости и эластичности важнейших инфраструктур.

Если рассматривать проблему защиты в перспективе, то можно отметить, что в настоящее время нации сталкиваются с диапазоном аморфных угроз их безопасности, и угрозы эти являются сложными в плане обеспечения безопасности с помощью традиционных инструментов и средств. Границы между внутригосударственным и иностранным, частным и общественным, полицией и вооруженными силами размываются, быстро меняются природа и требования национальной безопасности. Следствием этих перемен в сфере защиты киберпространства является то, что национальная политика для успешной борьбы с киберугрозой должна корректироваться с учетом растущей взаимозависимости экономик и необходимости межгосударственного сотрудничества.

Everywhere: A Research Agenda for Networked Systems of Embedded Computers, National AcademyPress, 2001

В.С. Разинкин

О скрытых формах терроризма

Научные исследования и правоприменительная практика показывает, что некоторые преступления, организуемые и совершаемые в рамках деятельности преступных организаций и сообществ в сфере потребительского рынка носят скрытый, законспирированный характер и по существу являются нелегальными террористическими акциями мошеннического типа, так называемый «торговый терроризм».

Оптовая и розничная торговля источниками радиоактивного излучения – сельскохозяйственной продукцией, товарами повседневного спроса и широкого потребления, имеющих высокий уровень радиации от 50 мк Р/час и выше, имеет высокие прибыли, ввиду низких закупочных цен, например в зонах радиоактивного заражения сельскохозяйственных и других земель зараженных радиацией при аварии на Чернобыльской АЭС, а также в субъектах Федерации результате слабого режима на объектах атомной промышленности и утечки радиации в атмосферу и на военных объектах по всей России. Скупщики, направляемые организаторами и руководителями преступных сообществ (преступных организаций) приобретают зараженный сильной радиацией товар почти за бесценок, а затем перепродают оптовым покупателям, либо организуют розничную торговлю на рынках крупных городов – мегаполисов (Москва, Санкт-Петербург, Нижний Новгород и другие), получая при этом высокую, а чаще всего сверхвысокую прибыль. Организаторы и руководители преступных сообществ не обращают внимание на тяжкие и особо тяжкие последствия от торговли радиоактивными источниками, выражающиеся в различных хронических заболеваниях, в том числе и в лучевой болезни и т.п. и т.д. Если же давать юридическую оценку в целом, грубейшим образом попирается экологический правопорядок и экологическая нравственость.

Действия членов преступных сообществ (преступных организаций) и их организаторов и руководителей подпадают под диспозицию части 3 статьи 205. Терроризм. УК РФ. Такие действия законодателем квалифицируются, как «иные действия создающие опасность гибели людей, причинения значительного имущественного ущерба, либо наступления иных общественно опасных последствий, если эти действия совершены в целях нарушения общественной безопасности»... Устрашения населения в рассматриваемом нами случае не будет ввиду того, что население не знает об опасных свойствах покупаемого товара. Не имеют причинной связи такие

действия с «оказанием воздействия на принятие решений органами власти» по вышеназванным обстоятельствам.

Термин «источники радиоактивного излучения» в УК РФ идентифицирован с терминами «радиоактивные отходы» или «опасные отходы». Согласно статьи 3 Федерального закона «Об использовании атомной энергии» в понятие радиоактивных отходов включаются не только не подлежащие дальнейшему использованию вещества и материалы, но и те изделия, оборудование, объекты биологического происхождения, в которых содержание радионуклеидов превышает уровни, установленные нормативными актами, исходя из Федерального закона «Об использовании атомной энергии».

Использование в торговле предметов продажи, являющихся источниками радиоактивного излучения, о чем знали заранее скупщики и организаторы и руководители преступных сообществ нарушает или покушается на общественную безопасность, ввиду того, что для них главная цель – получить высокую прибыль, в том числе и с риском привлечения к уголовной, административной и финансовой ответственности, а общественная безопасность для них ничего не значащее понятие.

Уголовный кодекс рассматривает общественную безопасность в качестве составного элемента большой группы общественных отношений, обеспечивающих не только общественную безопасность в узком смысле слова, но также общественный порядок, здоровье населения, общественную нравственность, экологический правопорядок и экологическую нравственность, безопасность движения и эксплуатацию транспорта, безопасность компьютерной информации. В соответствии с законом общественная безопасность в узком смысле слова есть совокупность общественных отношений, обеспечивающих безопасные условия жизни каждого члена общества, общественный порядок, безопасность личных, общественных или государственных интересов при производстве различного рода работ и в процессе обращения с общеопасными предметами (См.: «Уголовное право России». Особенная часть. Учебник под редакцией проф. А.И. Рарога. 3-ье издание. М., с. 221, 222). В нашем примере грубейшим образом нарушаются правила обращения с источниками радиоактивного излучения при производстве такого рода работ как заготовка сельхозпродуктов и торговля.

Торговля источниками радиоактивного излучения, путем скупки и перепродажи в крупных размерах, с целью получения высоких и сверхвысоких прибылей и доходов, не только покушается на здоровье населения, но и наносит ущерб экологической нравственности и экологическому правопорядку, следовательно скрыто, но беспрецедентно нарушается общественная безопасность, то есть налицо имеется состав преступления, предусмотренный статьей 205, ч.3 УК РФ.

Организаторы и руководители преступных сообществ (преступных организаций), зная об этом, и, идя на получение высоких и сверхвысоких прибылей, скупая и торгуя сельхозпродуктами и другими товарами, имеющими высокий радиоактивный фон совершают тем самым так называемый «торговый терроризм» с прямым умыслом.

Одним из основных признаков преступных сообществ (преступных организаций) является криминально-коммерческая деятельность, в том числе так называемый «торговый терроризм», в результате которой организаторы и руководители преступных сообществ имеют высокий доход или сверхдоход. Если криминально-коммерческая деятельность не получается и высоких доходов нет, то разложение преступных сообществ (преступных организаций) неизбежно. То есть преступные сообщества как в криминологическом, так и в уголовно правовом смысле это преступно-коммерческий, криминально-промышленный синдикат или картель, со всеми вытекающими криминально-экономическими последствиями, на что указывалось нами ранее.(См.: «Криминология». Учебник для юридических вузов. Под общей редакцией проф. А.И. Долговой. Издательская группа: «ИНФРА.М – НОРМА), Москва, 1997, с.605)

Организаторы и руководители преступных сообществ, имея высокие криминальные доходы, получили возможность с помощью приватизированных средств массовой информации, журналистов и писателей, находящихся на их содержании и довольствии, морализировать тяжкие и особо тяжкие преступления, асоциальный образ жизни, более изощренно пропагандировать негативные обычаи и традиции преступной среды, развенчивая при этом правоохранительные и другие государственные органы не только внутри страны, но и на международной арене, а также компрометировать криминальных и иных конкурентов, создавая благоприятные легально-правовые условия для дальнейшего получения высоких и сверхвысоких доходов и массированного проникновения в высшие эшелоны власти. Этому способствует высокий уровень коррупции в правоохранительной системе и других государственных органах.

Организаторы и руководители преступных сообществ полагают указанными и иными методами и способами оптимально интегрироваться с государственным аппаратом для создания криминально-государственного конгломерата мафиозного типа, для более глубокого внедрения в транснациональные преступные сообщества других государств и укрепления на рынке международной организованной преступности.