ТЕРРОРИЗМ В СОВРЕМЕННОМ МИРЕ

С.Г. ТУРОНОК

Информационный терроризм: выработка стратегии противодействия

Цель анализа – идентификация технологий, имеющих наибольший потенциал с точки зрения их применения террористическими организациями, а также выработка рекомендаций для сил безопасности, направленных на противодействие, предотвращение либо снижение эффективности применения террористами данных технологий.

Ключевые слова: терроризм, информационные и коммуникационные технологии, стратегия и тактика, рекрутирование, планирование и таргетирование, антитеррористическая деятельность.

The analysis purpose is identification of the technologies having the greatest potential from the point of view of their application by the terrorist organizations and development of recommendations for a safety force directed on counteraction, prevention or reduction of efficiency of application by terrorists of the given technologies.

Keywords: terrorism, information and communication technologies, strategy and tactics, planning and targeting, recruiting, antiterrorist activities.

В последние десятилетия широкое внедрение современных информационных технологий во все сферы общественной жизни существенно повысило зависимость общества, каждого конкретного индивида от надежности функционирования информационной инфраструктуры, достоверности используемой информации, ее защищенности от несанкционированной модификации, а также от противоправного доступа к ней. Возможности использования новых технологий в деструктивных, преступных и антисоциальных целях становятся все более актуальными, привлекают внимание представителей разных научных дисциплин и профессиональных сообществ. При этом сохраняется беспрецедентный разрыв между ускоряющимся темпом технологических инноваций и изменений, с одной стороны, и хронически запаздывающей реакцией политических и законотворческих институтов – с другой.

Сегодня ни у кого не вызывает сомнений тот факт, что террористические организации используют широкий спектр новейших технологий в процессе планирования и осуществления своих акций. Следует учитывать и то, что глобальный потребительский спрос на все новые виды продукции и их функциональные возможности порождает

Туронок Станислав Генрихович – кандидат политических наук, доцент кафедры политического анализа факультета государственного управления Московского государственного университета им. М.В. Ломоносова.

волну новых технологий, многие из которых могут быть применены террористами в целях повышения эффективности и результативности их акций. Вместе с тем технологии представляют собой обоюдоострое оружие: способствуя повышению эффективности и результативности, они в то же время могут создавать новые уязвимости. Изучение места и роли соответствующих технологий в структуре деятельности террористических организаций предполагает, таким образом, понимание не только природы самих технологий, но также целей и способов их применения в рамках конкретных оперативных действий террористов и противодействий сил безопасности.

Информационный терроризм, кибертерроризм – к определению понятий

Информационный терроризм за последние два десятка лет превратился в одно из наиболее опасных проявлений высокотехнологического терроризма, а информационные технологии стали его новой базой. Исследователи М. Девост, Б. Хьютон, Н. Поллард определяют информационный терроризм как сознательное злоупотребление цифровыми информационными системами, сетями или компонентами этих систем или сетей в целях, которые способствуют осуществлению террористических операций или актов (см. [Томас, 2002]).

Термин *кибертерроризм*, в свою очередь, ввел в середине 1980-х гг. сотрудник американского Института безопасности и разведки Б. Коллин, и обозначал он террористические действия в виртуальном пространстве. Тогда этот термин использовался лишь для прогнозов на будущее. Сам автор термина предполагал, что о реальном кибертерроризме можно будет говорить не раньше, чем в первые десятилетия XXI в.

Трудности в определении понятия кибертерроризма связаны с тем, что порой очень сложно отделить сам кибертерроризм от акций информационной войны, информационного оружия либо информационного криминала или преступлений в сфере компьютерной информации. Дополнительные трудности могут возникнуть при попытке выявить специфику данной формы терроризма. Например, психологический и экономический аспекты кибертерроризма тесно переплетены, и невозможно однозначно определить, какой из них имеет большее значение. Эта неопределенность говорит о новизне явления.

Киберпреступность (информационный криминал) – действия отдельных лиц или групп, направленные на взлом системы защиты, на хищение или разрушение информации в корыстных или хулиганских целях. Это, как правило, разовые преступления против конкретного объекта киберпространства. Преступление, совершенное в киберпространстве, – 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. Ключевым отличительным признаком киберпреступности принято считать корыстный характер действий злоумышленника.

Информационный терроризм (кибертерроризм), по мнению Е. Старостиной, отличается от указанных форм воздействия на киберпространство прежде всего своими целями, свойственными политическому терроризму вообще. Средства осуществления информационно-террористических действий могут варьироваться в широких пределах и включать все виды современного информационного оружия. В то же время тактика и приемы его применения существенно отличаются от тактики информационной войны и приемов информационного криминала. Кибертеррорист отличается от хакера, компьютерного хулигана или компьютерного вора, которые действуют в корыстных или хулиганских целях. Главное в тактике информационного терроризма состоит в том, чтобы террористический акт имел опасные последствия, стал широко известен населению и получил большой общественный резонанс. Как правило, передаваемые в СМИ требования сопровождаются угрозой повторения акта без указания конкретного объекта.

Старостина предлагает следующее определение кибертерроризма: "…это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающая опасность для жизни или здоровья людей или наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта" [Старостина]. При этом исследователь квалифицирует кибертерроризм как разновидность киберпреступности.

Д. Деннинг, профессор Джорджтаунского университета и один из самых авторитетных экспертов в области компьютерной преступности и кибербезопасности в книге "Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику" говорит о кибертерроризме как о "противоправной атаке или угрозе атаки на компьютеры, сети или информацию, находящуюся в них, совершенной с целью принудить органы власти к содействию в достижении политических или социальных целей" [Denning, с. 48]. По мнению Е. Роговского, следуя этим определениям, можно выделить два вида кибертерроризма:

– непосредственное совершение террористических действий с помощью компьютеров и компьютерных сетей;

– использование киберпространства террористическими группами в организационно-коммуникационных целях и с целью шантажа, но не для непосредственного совершения терактов [Роговский].

Первый вид соответствует объединению понятий "киберпространство" и "терроризм" и представляет собой умышленную атаку на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающую опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. Например, перехват управления военным или инфраструктурным объектом в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти путем угрозы осуществления аварии (катастрофы) [Тропина; Голубев]. К первому виду кибертерроризма примыкают все осуществляемые с помощью Интернета так называемые "информационные" правонарушения против конституции (антиконституционные призывы, угрозы конституционным правам и свободам человека и гражданина, распространение устрашающих слухов, угрозы информационному обеспечению государственной политики и др.).

Второй вид кибертерроризма – использование информационного пространства террористическими группами в организационно-коммуникационных целях (но не для непосредственного совершения терактов), проведение теоретического, военного, теологического обучения и пропаганды, а также рекрутирование новых членов и обеспечение связи между отдельными ячейками. Существует несколько способов, с помощью которых террористические группы используют Интернет в своих целях:

– сбор информации, необходимой для планирования терактов;

– сбор денег для поддержки террористических движений (в том числе, путем вымогательства и шантажа);

– распространение агитационно-пропагандистской информации о террористических движениях, их целях и задачах, намеченных действиях, формах протеста, обращение к массовой аудитории с сообщениями о признании своей ответственности за совершенные террористические акты и т.п.;

– информационно–психологическое воздействие на население с целью шантажа, создания паники, распространения дезинформации и тревожных слухов;

– организационная деятельность: например, размещение в открытом доступе и рассылка открытых и зашифрованных инструкций (информации о взрывчатых веществах и взрывных устройствах, ядах, отравляющих газах, а также инструкций по их самостоятельному изготовлению), сообщений о времени встреч заинтересованных людей и проч.;

– анонимное привлечение к террористической деятельности соучастников, например хакеров и представителей бизнеса, оказывающих различные информационные услуги на коммерческой основе и не отдающих себе отчета в том, кто и почему эти услуги оплачивает;

– возрастающие технологические возможности применения коммуникационных технологий для планирования и координации своих действий, что создает основу для перехода к менее четким организационным структурам, расширения потенциала малых террористических групп, намеренных осуществлять свои операции децентрализовано [Роговский].

Инновационные практики и формы адаптации современных технологий в деятельности террористических организаций

В качестве первого шага к пониманию интересующей нас проблематики необходимо выработать структурированное представление о функционировании террористической организации, деятельность которой отнюдь не сводится непосредственно к террористическим акциям как таковым. Речь идет о широком спектре организационных функций и видов деятельности, обеспечивающих жизнеспособность террористической организации в широком смысле слова. Наиболее характерные виды деятельности, присущие большинству террористических групп, могут быть представлены в виде следующей фазовой модели террористической активности (см. рис.).

Анализируя практику применения террористами сетевых технологий на каждой из выделенных фаз, с учетом ожидаемых возможностей новых технологий в будущем можно установить, какие виды деятельности террористических организаций способны в наибольшей степени выиграть от применения этих технологий и какие конкретные технологии сулят наибольший эффект от их применения. Ответ на этот вопрос предполагает анализ того, как террористы применяли сетевые технологии в прошлом, применяют их в настоящее время и каковы перспективы применения их в будущем, следует ли ожидать в этой связи качественных изменений в тех или иных видах деятельности террористических организаций?

Следующий шаг предполагает идентификацию конкретных сетевых технологий, которые могут представлять наибольший интерес для конкретного вида террористической активности, насколько практичным и эффективным будет приобретение данной технологии, и способна ли она привнести революционные изменения в существующую практику. Моя оценка опирается на допущение, согласно которому обращение террористов к той или иной технологии оправдано, если способно обеспечить им один из двух типов преимуществ при допустимом уровне риска:

– преимущества, обеспечивающие повышение способностей террористической организации в осуществлении конкретных видов ее деятельности в стратегическом плане (например, рекрутирование или обучение);

– преимущества, обеспечивающие повышение результативности террористических атак в тактическом плане (например, повышающие летальность атак либо снижающие риск обнаружения и возмездия в отношении участников).

Исторически **рекрутирование** в террористических организациях оставалось скрытым, глубоко законспирированным видом деятельности. В условиях подпольного существования и господствующего общественного осуждения целей и средств террористической деятельности скрытность была необходимым условием выживания организации, что, в свою очередь, определяло преобладание контакта “лицом к лицу”. В таких условиях создаются определенные ограничения, сужающие потенциальную аудиторию. Индивидуальный тип рекрутирования в сочетании с необходимостью соблюдения скрытности и безопасности требует более длительного процесса, предполагающего также изощренную процедуру испытания и проверки рекрута. Таким

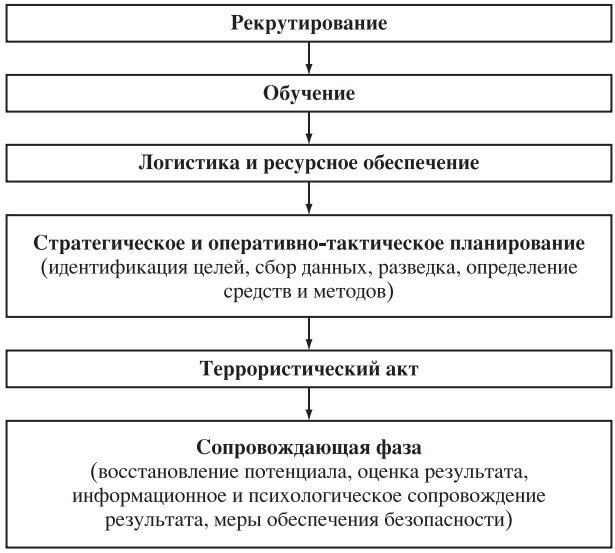

Рис. Основные виды деятельности террористической организации.

образом, сами формы и методы рекрутирования предопределяли локальный масштаб такой активности и ограниченный круг потенциальных рекрутов.

Сегодня формы и методы рекрутирования, опирающиеся на новые сетевые технологии, значительно увеличили масштаб, эффективность и результативность данного вида деятельности. Во-первых, рекрутирование может осуществляться дистанционно. С учетом практически повсеместной доступности соответствующих материалов в Интернете, традиционный контакт "лицом к лицу" становится не нужен. При этом задачи рекрутирования облегчаются за счет того, что более широкие аудитории могут узнать о существовании и целях той или иной организации. Во-вторых, современные формы дистанционного рекрутирования более эффективны благодаря тому, что один рекрутер имеет возможность "разрабатывать" одновременно большое число людей, проживающих не только в пределах его региона, страны, но также в отдаленных концах мира. Современные сетевые технологии, такие как Интернет и видеоигры, повышают возможности террористических групп распространять и пропагандировать свои идеи, в том числе учитывая проблемы адаптации формы и содержания послания к особенностям конкретных целевых аудиторий. В частности, Хесболлах использовала самодельные видеоигры с элементами насилия и жестокости, такие как Special Force и Under Ash, в целях пропаганды своих пропалестинских и антиизраильских взглядов и привлечения потенциальных кандидатов в Ливане и в других странах [Lewis, 2005, p. 11].

Технический прогресс значительно видоизменил практику **ресурсного обеспечения** террористических организаций. Инновационные финансовые инструменты, такие как киберплатежи и Интернет-банкинг, а также отмывание денег и другие финансовые киберпреступления становятся в последние годы все более доступны и для террористов [Wilson, Roger, 1998]. Имеются примеры применения террористами компьютерного оборудования для взлома и создания кредитных карт, использования электронных переводов в целях конспирации и снижения рисков, связанных с физическим контактом. Речь идет также об использовании неформальных платежных сетей, выключенных из официальных финансовых систем, таких как *hawala* ("доверие" – *хинди*). Подобные финансовые трансферты не оставляют юридически значимых "следов" и обеспечивают анонимность как отправителю, так и получателю средств [Money… 2004]. Для террористов они предоставляют уникальную возможность осуществлять глобальные финансовые операции при минимальных издержках и минимальном риске.

Сетевые технологии также значительно облегчают задачу пропаганды как составной части процесса фандрайзинга. Так, некоторые исламские новостные каналы публикуют призывы к своей аудитории осуществлять добровольные пожертвования; счета трех международных "благотворительных" фондов, активно действующих в Интернете, – Benevolence International Foundation, The Global Relief Foundation и Al-Haramain Foundation, – были заморожены властями США по подозрению в связях с Аль-Каидой [Weimann, 2004, p. 128].

При применении современных технологий существуют как новые возможности, так и новые уязвимости. Тем не менее, несмотря на имеющиеся риски и ограничения, электронные финансовые трансферты, по оценкам экспертов, сулят поистине революционные изменения в практике деятельности террористических групп, поскольку предоставляют им не имеющий аналогов доступ к финансовым ресурсам единомышленников, находящихся за пределами страны их пребывания.

В зависимости от конечных целей и уровня развития террористической организации потребности в **обучении и тренинге** могут варьировать от начальной подготовки в обращении с легким стрелковым оружием и взрывчаткой, до высокоспециализированного обучения оперативно-тактическим действиям и процедурам, включающим применение высоких технологий.

Развитие и распространение Интернета привело к появлению огромной и динамически пополняемой онлайновой библиотеки обучающих материалов на множестве языков народов мира, не только охватывающих различные виды вооружения, техники и методики проведения террористических атак, но также предоставляющих подробные инструкции по обеспечению скрытности и безопасности их участников [Coll, Susan, 2005; Taylor, 2005]. Видео в последнее время превращается в один из ключевых компонентов технологического обучения. За последнее десятилетие производство и применение видеозаписей в террористической деятельности значительно возросло. Такие записи используются не только в процессе оперативного обучения боевиков, но также в других целях: как элемент пропаганды, как средство оценки причиненного ущерба и общей эффективности проведенной операции, как способ изучения реакции силовых структур в целях совершенствования и выработки новой террористической тактики.

Отмечены случаи применения террористами средств компьютерной симуляции и связанных с ними программных технологий в процессе подготовки к проведению акции. Так, участники теракта 11 сентября 2001 г., управлявшие захваченными самолетами, использовали в своей подготовке программу-симулятор Боинга 747-400, а также обучающую видеозапись действий пилота Боинга 767 [National… 2004, p. 168]. Очевидно, применение подобных средств обеспечивает несравнимо более эффективную подготовку с соблюдением скрытности в сравнении с любыми практическими тренировками в условиях, приближенных к реальным.

Оперативно-тактическое планирование. Как свидетельствует история, эффективные террористические группы несколько лет вкладывали немалые усилия и средства в разведку, рекогносцировку и таргетирование. Конечно, есть и примеры успешных атак, осуществленных без предварительной разведки и рекогносцировки. В прошлом террористические группы осуществляли эти виды деятельности с минимумом технических средств, а полученная подобным образом информация использовалась в сравнительно простых формах планирования.

Современные сетевые технологии внесли существенные изменения в данные виды деятельности, значительно расширили возможности ведения разведки и рекогносцировки. Доступные и миниатюрные цифровые фото- и видеокамеры облегчают задачу скрытой фиксации происходящего; получаемые изображения не нуждаются в процедуре проявки, что позволяет избавиться от громоздкого оборудования, способного привлечь внимание посторонних; их также легко отредактировать и обработать с помощью компьютера. Более продвинутые террористические группы могут извлечь пользу из спутниковых снимков коммерческого назначения, навигационной системы GPS, а также обширной информации об интересующих их объектах, доступной в

Интернете; эта информация может быть получена на анонимной основе при минимуме усилий. Подобные возможности позволяют существенно повысить эффективность разведывательной деятельности, не подвергая при этом угрозе членов группы. Кроме того, разведчики, действующие на местности, способны практически мгновенно пересылать полученную информацию для дальнейшей обработки и анализа в штаб, расположенный в другом конце мира, используя при этом доступные средства шифрования данных, снижая тем самым риск обнаружения и применения контрразведывательных мер.

Основания для беспокойства внушает наблюдаемая тенденция миниатюризации и удешевления технологий, пригодных для осуществления данных видов деятельности. Этот фактор упрощает доступ террористов к интересующим их технологиям. Кроме того, эффективность разведывательных данных повышается по мере увеличения их точности (разрешения) в сочетании с простотой и легкостью их доставки лицам, осуществляющим анализ и планирование. Также следует обратить внимание на расширение доступа к средствам шифрования, что снижает риски обмена электронной информацией (в том числе цифровым видео и фото) между организаторами и исполнителями террористических акций.

Революционные технологические изменения, имеющие отношение к планированию террористических акций, в будущем способны значительно ускорить этот процесс, позволяя террористическим группам осуществлять в течение нескольких дней или недель серии терактов, на подготовку которых в прошлом могли уходить месяцы и годы. Выход на подобный уровень возможностей, скорее всего, потребует освоения методов симуляции и моделирования, внедрения защищенных средств коммуникаций, систем поддержки принятия решений и др.

Террористические акты, как правило, разыгрываются на “сцене”, обращенной к одной или нескольким аудиториям. В отличие от акций партизанской войны или диверсионных операций, акты террора обычно представляют минимальную ценность с военной точки зрения, в то же время для них исключительно важен месседж, обращенный к целевой аудитории. Содержанием месседжа может быть привлечение внимания к фактам исторической несправедливости, демонстрация силы или дискредитация власти. Речь идет о **пропаганде и убеждении**, представляющих собой один из ключевых элементов террористического акта. Современные инструменты пропаганды могут включать заснятые на камеру мобильного телефона сцены насилия, любительские видеоклипы и профессиональные постановочные фильмы с изложением требований и идеологических принципов террористической группы наряду с традиционными пропагандистскими материалами, такими как заявления об ответственности, обращения лидеров террористических организаций, и т.д.

В настоящее время современные сетевые технологии, а также инновационные коммерческие и социальные формы их применения существенным образом повлияли на возможности террористических групп предпринимать пропагандистские и информационные операции, нацеленные на массовую аудиторию. Значительно возросло многообразие доступных медиаресурсов. Если в прошлом террористы были ограничены выбором между телевидением, радио, печатной продукцией, граффити и подобными им, то сегодня они могут воспользоваться широкими возможностями Интернета для организации веб-сайтов, электронных журналов, радиоканалов и иных средств онлайн коммуникации [Zanini, Sean, 2001]. Как отмечает в этой связи американский исследователь Г. Вейманн, “Аль-Каида сочетает возможности мультимедийной пропаганды и передовых коммуникативных технологий, результатом чего оказывается весьма изощренная форма психологической войны” [Weimann, 2004, p. 79]. Помимо этого, сегодня не составляет труда произвести высококачественные, близкие к профессиональным пропагандистские материалы, используя доступное программное обеспечение и недорогое компьютерное оборудование. Современные программные приложения значительно облегчают задачу перевода материалов на иностранные языки. Мультимедийная продукция, содержащая видеоматериал, может даже не нуждаться в переводе.

Наконец, в настоящее время осуществление контрпропагандистских мер в рамках антитеррористической деятельности становится все сложнее. Утратив прежние возможности эффективно ограничивать распространение террористической пропаганды и контролировать содержание независимых информационных ресурсов, государство оказывается перед необходимостью противодействия террористической пропаганде посредством собственных информационных кампаний, что представляет собой заметный сдвиг в динамике конфликта между террористами и антитеррористическими силами. Речь идет о новой форме соревнования, к которой государственные деятели и соответствующие структуры не в полной мере готовы. При этом любой специалист в области организации политических кампаний подтвердит очевидный факт: само по себе публичное упоминание террористической пропаганды неизбежно повышает ее видимость для широкой аудитории, а следовательно, и ее влияние.

Стратегия противодействия применению террористами новых технологий

Идентификация способов и методов противодействия подобной практике – задача более сложного порядка в сравнении с выявлением технологий, представляющих потенциальный интерес для террористических организаций. Руководящим принципом в решении этой задачи может служить совокупный вклад предлагаемой меры противодействия в повышение результативности антитеррористической деятельности государства. В целях всесторонней оценки возможных мер противодействия силы безопасности должны не только ясно представлять риски и выгоды, связанные с самим фактом овладения террористами той или иной технологией, но также возможные риски и выгоды, возникающие вследствие использования рассматриваемых мер противодействия. Характеризуя альтернативные варианты мер противодействия использованию террористическими организациями новых сетевых технологий, можно структурировать проблемное поле по следующим четырем измерениям.

1. *Практики, предполагающие отказ в доступе.* Отказ террористам в доступе к новым технологиям посредством прямых (нормативных) ограничений на распространение определенного технологического оборудования либо иного противодействия террористическим группам в получении доступа к конкретной технологии, на первый взгляд, может казаться вполне жизнеспособной альтернативой. На деле же подобный подход представляется весьма проблематичным, особенно там, где террористы полагаются на широкий выбор продуктов, предлагаемых потребительским рынком, либо используют гибкие технологии, исправно работающие в большинстве случаев, в том числе в условиях активных контрмер. Запретительные меры можно квалифицировать как нереалистичные применительно к большинству ситуаций, за редким исключением тех, где речь идет о строго секретных, закрытых разработках, не предназначенных для коммерческого использования.

2. *Практики, предполагающие создание препятствий в применении технологии.* Технические контрмеры, такие как глушение каналов связи или вывод из строя террористических веб-сайтов посредством вредоносных программных продуктов, хорошо известны и имеют обширный опыт применения, их результативность достаточно высока особенно там, где речь идет о сетевых технологиях коммерческого назначения. В то же время не вполне очевиден остается баланс выгод и рисков осуществления таких контрмер, не в последнюю очередь из-за высокой вероятности ущерба для законопослушных пользователей. Суть проблемы видится в том, что борьба против террористических групп разыгрывается в сфере открытого общества, а не в границах замкнутого поля боя. В результате технические контрмеры, которые можно было бы признать наиболее эффективными, должны быть одновременно наиболее избирательными в своем действии, то есть сводящими к минимуму побочные последствия. Коротко говоря, способ противодействия применению террористами новых технологий, предполагающий прямые технические контрмеры, непосредственно нацеленные на

работоспособность соответствующего оборудования либо программного обеспечения, может быть результативным лишь в определенных ситуациях и обстоятельствах.

3. *Практики, предполагающие скрытую эксплуатацию технологических уязвимостей.* Полагая конечной целью сил безопасности нанесение террористическим группам поражения в долгосрочной перспективе, можно попытаться превратить тенденцию применения террористическими организациями новых сетевых технологий в фактор стратегического преимущества для сил безопасности, способных эксплуатировать скрытые технологические уязвимости и дефекты для получения критически значимой информации, облегчающей осуществление мер прямого действия против террористов (аресты, акции возмездия и т.д.).

Следует учитывать, что какой бы мощной и жизнеспособной ни выглядела та или иная террористическая организация, ее отдельные звенья могут оставаться весьма уязвимыми. Чем активнее отдельные звенья вовлекаются в сетевые коммуникации и формы активности, тем дальше они заходят за "красную черту", ограничивающую область внутренней безопасности организации, в пределах которой персонал, оборудование, программное обеспечение, средства коммуникации и иные оберегаемые ресурсы находятся под неусыпным оком специалистов в области безопасности.

Силы безопасности, используя свои политико-административные ресурсы, зачастую имеют возможность обеспечить появление на потребительском рынке моделей мобильных телефонов, компьютеров и иных аппаратных или программных продуктов, в которые производителем заблаговременно встроены скрытые возможности для удаленного доступа и съема интересующей информации. "Непрозрачное" (в представлении не прошедшего специальную подготовку пользователя) функционирование многих современных технологий и устройств значительно облегчает задачу скрытного доступа и контроля со стороны спецслужб.

4. *Практика, предполагающая непротиводействие.* Нельзя однозначно исключить и логику, стоящую за отказом от проведения каких-либо мер противодействия использованию террористами новых технологий, в пользу концентрации имеющихся ресурсов на иных уязвимых сторонах деятельности террористических организаций. Такой вариант может быть достаточно рациональным в случаях, когда есть основания ожидать незначительный эффект от применения террористами новых технологий в своей деятельности, либо если такой эффект не имеет очевидной взаимосвязи именно с технологическим фактором.

* * *

В целом, как было отмечено выше, проведенный анализ показывает низкую степень вероятности каких-либо подлинно революционных изменений в существующем балансе сил между терроризмом и современным государством, которые можно было бы приписать появлению существующих либо гипотетических технологий. Тем не менее отдельные технологии, рассмотренные здесь, представляют известный потенциал изменений, способный при определенной комбинации условий оказать существенное воздействие на политику безопасности.

С точки зрения сил безопасности, необходимо осуществлять постоянный мониторинг развития данных технологий. В случае появления новой информации, свидетельствующей о значительном прогрессе в разработке и распространении подобных технологий, дополнительные ресурсы сил безопасности должны быть направлены на реализацию комплекса мер, препятствующих овладению террористическими организациями этими технологиями.

Между тем существенно иная ситуация имеет место в отношении применения террористами технологий, обладающих свойством *универсальности* применения либо *представленных многообразием образцов потребительского рынка*. Анализ свидетельствует, что в данном случае речь может идти о незначительных изменениях в плане результативности террористических операций; в то же время можно ожидать

заметных эффектов с точки зрения совокупной эффективности функционирования террористических организаций, что позволит небольшим группам осуществлять более масштабные кампании террора. Также характерной чертой указанной категории технологий следует признать низкую степень результативности мер противодействия, предполагающих отказ в доступе (если таковые вообще могут быть практически реализованы).

В то же время в этом случае меры эксплуатации скрытых уязвимостей и дефектов технологий, используемых террористами, способны дать положительные результаты. Поскольку данная категория технологий, как правило, имеет отношение к процессам сбора, хранения, распространения и модификации информации, порой критически значимой с точки зрения компрометации соответствующей группы, выгоды от эксплуатации скрытых уязвимостей как элемент антитеррористической деятельности могут значительно перевешивать соответствующие риски, связанные с использованием данных технологий террористами.

Представленный анализ предполагает, что стратегия противодействия применению террористами новых технологий должна быть сконцентрирована по преимуществу на тех технологиях, которые сулят приращение совокупной эффективности деятельности террористических организаций в сравнении с теми, что ориентированы на конечную результативность террористических акций. Усилия и ресурсы, ориентированные на гипотетический "революционный" потенциал сетевых технологий, должны быть сосредоточены в первую очередь на мерах мониторинга и раннего оповещения по поводу практики разработки и применения подобных технологий, нежели на мерах прямого противодействия технологиям как таковым.

СПИСОК ЛИТЕРАТУРЫ

Голубев В.А. Кибертерроризм как новая форма терроризма? (http://www.crime-research.org).

Роговский Е.А. Россия в борьбе с международным терроризмом: грани повышения позитивного образа страны // Россия и Америка в XXI веке. Интернет-издание.

Старостина Е. Терроризм и кибертерроризм: угроза международной безопасности // Центр исследования компьютерной преступности. Интернет-издание (www.crime-research.ru).

Томас Т.Л. Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху // Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции. М., 2002.

Тропина Т. Киберпреступность и кибертерроризм (http://www Crime.vl.ru).

Coll S., Susan B.G. Terrorists Turn to the Web as Base of Operations // The Washington Post. August 7, 2005.

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).

Lewis N. Dangerous Games: how the Seductive Power of Video Games Is Being Harnessed to Push Deadly Agendas // The Calgary Herald. July 9, 2005.

Money-Transfer Systems, Hawala Style // CBC News Online. June 11, 2004.

National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States. New York, 2004.

Taylor P. The New Al-Qaeda: Jihad.com // BBC Television. July 20, 2005.

Weimann G. Www.Terror.Net: how Modern Terrorism Uses the Internet. Washington (D.C.), March 2004.

Wilson P., Roger C.M. Exploring Money Laundering Vulnerabilities Through Emerging Cyberspace Technologies: a Caribbean-based Exercise. Santa Monica (Cal), 1998.

Zanini M., Sean J.A.E. The Networking of Terror in the Information Age // Networks and Netwars: the Future of Terror, Crime, and Militancy. Santa Monica (Cal), 2001.