UNODC

Управление Организации Объединенных Наций
по наркотикам и преступности

Использование Интернета

в террористических целях

В сотрудничестве
С ЦЕЛЕВОЙ ГРУППОЙ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ОСУЩЕСТВЛЕНИЮ КОНТРТЕРРОРИСТИЧЕСКИХ МЕРОПРИЯТИЙ

УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО НАРКОТИКАМ И ПРЕСТУПНОСТИ
Вена

ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА В ТЕРРОРИСТИЧЕСКИХ ЦЕЛЯХ

ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ
Нью-Йорк, 2013 год

Употребляемые обозначения и изложение материала в настоящем издании не означают выражения со стороны Секретариата Организации Объединенных Наций какого бы то ни было мнения относительно правового статуса какой-либо страны, территории, города или района или их властей или относительно делимитации их границ.

Содержащиеся в настоящей публикации унифицированные указатели ресурсов и ссылки на интернет-сайты указаны для удобства читателей и являются действительными на момент издания публикации. Организация Объединенных Наций не несет ответственности за сохранение достоверности этой информации, равно как и за содержание любого внешнего веб-сайта.

Подготовка к изданию: Секция английского языка и издательских и библиотечных услуг, Отделение Организации Объединенных Наций в Вене.

"Интернет является наглядным примером того, как террористы могут действовать действительно на транснациональной основе; в ответ государствам необходимо думать и действовать на столь же транснациональной основе".

Пан Ги Мун

Генеральный секретарь Организации Объединенных Наций

Предисловие

Директор-исполнитель Управления Организации Объединенных Наций по наркотикам и преступности

Использование Интернета в террористических целях представляет собой быстро расширяющееся явление, которое требует принятия активных и скоординированных ответных мер со стороны государств-членов.

В рамках реализации своего мандата, направленного на укрепление потенциала национальных систем уголовного правосудия в плане осуществления положений международно-правовых документов по борьбе с терроризмом, Управление Организации Объединенных Наций по наркотикам и преступности (ЮНОДК) играет ключевую роль в оказании помощи государствам-членам и делает это в соответствии с принципами верховенства права и международными нормами в области прав человека. В частности, в 2011 году Генеральная Ассамблея в своей резолюции 66/178 вновь подтвердила мандат ЮНОДК, состоящий в том, чтобы продолжать наращивать специализированные юридические знания в области противодействия терроризму и соответствующих тематических областях, включая использование Интернета в террористических целях.

Несмотря на растущее в последние годы международное признание угрозы, которую несет с собой использование террористами Интернета, в настоящее время не существует универсального инструмента, специально посвященного этому приобретающему все более значительные масштабы направлению террористической деятельности. Кроме того, доступные возможности специализированной подготовки персонала по правовым и практическим аспектам расследования связанной с использованием Интернета деятельности террористов и судебного преследования за нее весьма ограниченны. Настоящая публикация служит дополнением к уже имеющимся ресурсам, разработанным ЮНОДК в таких областях, как борьба с терроризмом, пресечение киберпреступности и обеспечение верховенства права. В ней также уделяется внимание важности накопления комплексных специальных знаний, необходимых для удовлетворения потребностей государств-членов в технической помощи в целях борьбы с этой постоянно нарастающей угрозой. ЮНОДК выражает глубокую признательность правительству Соединенного Королевства Великобритании и Северной Ирландии за великодушную поддержку, сделавшую возможной публикацию этой работы.

Настоящее издание, предназначенное для использования как в качестве самостоятельного ресурса, так и в рамках поддержки инициатив ЮНОДК по созданию потенциала, призвано служить руководством по существующим на сегодняшний день нормативно-правовым базам и практике на национальном и международном уровнях, связанным с криминализацией, расследованием и судебным преследованием террористической деятельности с использованием Интернета.

Терроризм во всех его проявлениях затрагивает всех нас. Для использования Интернета в процессе осуществления террористических целей не существует национальных границ, вследствие чего усиливается потенциальное воздействие на жертв. Освещая конкретные случаи и передовой опыт в области ответных мер в связи с этим уникальным вызовом, настоящая публикация имеет две цели: во-первых, способствовать лучшему пониманию тех способов, с помощью которых коммуникационные технологии могут злонамеренно использоваться в целях содействия совершению актов терроризма, и, во-вторых, добиться расширения сотрудничества между государствами-членами в деле разработки эффективных мер в области уголовного правосудия в ответ на эту транснациональную проблему.

Юрий Федотов

Директор-исполнитель
Управления Организации Объединенных Наций по наркотикам и преступности

Целевая группа Генерального секретаря по осуществлению контртеррористических мероприятий

Деятельность Рабочей группы по противодействию использованию Интернета в террористических целях в рамках Целевой группы по осуществлению контртеррористических мероприятий направлена на координацию действий системы Организации Объединенных Наций в поддержку Глобальной контртеррористической стратегии Организации Объединенных Наций, принятой Генеральной Ассамблеей в своей резолюции 60/288, в которой государства-члены вынесли решение о "координации усилий, предпринимаемых на международном и региональном уровнях в целях борьбы с терроризмом во всех его формах и проявлениях в сети Интернет" и "использовании сети Интернет в качестве инструмента борьбы с распространением терроризма, признавая при этом, что государствам может потребоваться помощь в этих вопросах". Рабочая группа определила три основные темы для обсуждения: правовые вопросы, технические вопросы и методы, посредством которых международное сообщество могло бы более эффективно использовать Интернет в борьбе с терроризмом и разоблачать несостоятельность утверждений террористов, будто насилие является законным способом осуществления политических перемен.

Настоящее исследование, подготовленное Управлением Организации Объединенных Наций по наркотикам и преступности и проводившееся в рамках Рабочей группы, во многом обязано содействию и поддержке государств-членов. Оно выводит обсуждение правовых проблем на новый уровень и существенно обогащает знания и опыт в этой области, накопленные Рабочей группой и используемые ею совместно с государствами-членами. В частности, в исследовании приводятся важные образцы законодательства государств-членов, касающегося использования Интернета террористами, и на примере реальных судебных дел демонстрируются трудности, с которыми государства-члены сталкиваются при криминализации таких актов и уголовном преследовании за их совершение.

Рабочая группа убеждена, что настоящий доклад поможет определить области законодательной деятельности, в которых Организация Объединенных Наций может оказать государствам-членам содействие в осуществлении Глобальной контртеррористической стратегии в процессе борьбы с таким явлением, как использование Интернета в террористических целях.

Ричард Баррет

Координатор Группы по аналитической поддержке и наблюдению за санкциями, Сопредседатель Рабочей группы по противодействию использованию Интернета в террористических целях при Целевой группе по осуществлению контртеррористических мероприятий

Правительство Соединенного Королевства

В течение последнего десятилетия Соединенное Королевство выступает инициатором принятия законодательства по противодействию использованию Интернета в террористических целях; мы добились значительных успехов в борьбе с деятельностью террористов в Интернете в пределах границ нашей страны, принимая все возможные меры для сохранения свобод и выгод, которые Интернет принес нашим гражданам.

Однако мы признаем, что данная угроза по природе своей носит транснациональный характер. У международного сообщества есть надежда эффективно решить проблему использования Интернета террористами, только действуя сообща.

В связи с этим правительство Соединенного Королевства приветствует возможность оказать поддержку ЮНОДК в выпуске данной публикации, которую вы собираетесь прочесть. Мы надеемся, что она вскоре станет полезным инструментом для законодателей, сотрудников правоохранительных органов и работников систем уголовного правосудия при разработке и применении нормативно-правовой базы, которая реально положит конец деятельности террористов в Интернете. Если это произойдет, то будет внесен важный вклад в дело превращения наших сообществ – как реальных, так и виртуальных – в более безопасное место.

Саймон Шерклифф

Начальник Оперативного отдела
по борьбе с терроризмом
Министерства иностранных дел
и по делам Содружества

Сью Хемминг

(офицер Ордена Британской империи)
Начальник Специального отдела
по борьбе с преступностью и терроризмом
Службы уголовного преследования

Содержание

История вопроса

Технологии являются одним из стратегических факторов, способствующих все более широкому использованию Интернета террористическими организациями и их сторонниками для решения широкого круга задач, включая вербовку, финансирование, пропаганду, подготовку исполнителей, подстрекательство к совершению актов терроризма, а также сбор и распространение информации в террористических целях. В то время как многие достоинства и преимущества Интернета очевидны, он также может использоваться для содействия связи внутри террористических организаций, а также в целях передачи информации о планируемых террористических актах и обеспечения их материальной поддержки, и для эффективного расследования таких преступлений необходимо располагать специальными техническими знаниями по каждому из этих правонарушений.

Согласно общепринятому принципу предполагаемым террористам, несмотря на одиозный характер их деяний, должны предоставляться такие же процессуальные гарантии в рамках уголовного права, как и любым другим подозреваемым. Защита прав человека является одной из основных ценностей Организации Объединенных Наций и основополагающим принципом подхода к борьбе с терроризмом с позиций верховенства права. Соответственно, в настоящей публикации подчеркивается важность неизменного соблюдения принципов прав человека и основных свобод, в частности в контексте разработки и реализации правовых документов, касающихся борьбы с терроризмом.

Управление Организации Объединенных Наций по наркотикам и преступности (ЮНОДК) в качестве подразделения Организации Объединенных Наций – ключевого в оказании правовой и связанной с ней технической помощи в целях борьбы с терроризмом – активно участвует в работе Целевой группы по осуществлению контртеррористических мероприятий, тем самым обеспечивая, чтобы деятельность ЮНОДК по борьбе с терроризмом велась в более широком контексте общих усилий всей системы Организации Объединенных Наций и в координации с ними. В январе 2010 года действующая в рамках Целевой группы Рабочая группа по противодействию использованию Интернета в террористических целях выступила инициатором проведения серии конференций с участием представителей правительств, международных и региональных организаций, аналитических центров, научных кругов и частного сектора для оценки использования Интернета в террористических целях и потенциальных возможностей борьбы с таким использованием. Цель инициативы Рабочей группы состояла в том, чтобы предоставить государствам-членам обзор текущего состояния данной проблемы и предложить политические установки, проекты и практические рекомендации по правовым, техническим аспектам проблемы, а также по воспитательно-просветительским мерам. Конференции Рабочей группы состоялись в январе 2010 года в Берлине, в феврале 2010 года в Сиэтле (Соединенные Штаты Америки) и в январе 2011 года в Эр-Рияде.

Во исполнение своего мандата, состоящего в том, чтобы "наращивать специализированные юридические знания в области противодействия терроризму... и оказывать государствам-членам, по их просьбе, помощь в принятии в рамках системы уголовного правосудия мер противодействия терроризму, включая... использование Интернета в террористических целях"[1], Сектор ЮНОДК по вопросам предупреждения терроризма совместно с Сектором ЮНОДК по организованной преступности и незаконному обороту и при поддержке правительства Соединенного Королевства Великобритании и Северной Ирландии взял на себя обязательство

[1] Резолюция 66/178 Генеральной Ассамблеи.

подготовить, в качестве вклада в реализацию проекта Рабочей группы, настоящее пособие по оказанию технической помощи в связи с использованием Интернета в террористических целях. Данная публикация ЮНОДК основана на выводах конференций Рабочей группы, в частности состоявшейся в январе 2010 года в Берлине конференции по правовым аспектам терроризма, непосредственно связанным с использованием Интернета.

В связи с подготовкой настоящей публикации ЮНОДК в октябре 2011 года и феврале 2012 года провело в Вене два совещания групп экспертов, для того чтобы предоставить работникам системы уголовного правосудия по борьбе с терроризмом из государств-членов, принадлежащих к разным географическим группам, трибуну для обмена опытом, который касается использования Интернета в террористических целях. В этих встречах приняли участие эксперты в общей сложности из 25 государств-членов, в том числе ответственные работники прокуратуры, сотрудники правоохранительных органов и научные сотрудники, а также представители ряда межправительственных организаций. В настоящей публикации широко используются материалы состоявшихся в ходе этих встреч обсуждений и обмена экспертным опытом, и она призвана оказать государствам-членам практическую помощь в целях содействия более эффективному расследованию и судебному преследованию по делам против террористов, связанным с использованием Интернета.

I. Использование Интернета в террористических целях

A. Введение

1. С конца 1980-х годов Интернет показывает себя как в высшей степени динамичное средство коммуникации, охватывающее неуклонно расширяющуюся аудиторию по всему миру. Разработка все более сложных технологий ведет к формированию сети поистине глобального масштаба, причем со сравнительно невысокими барьерами для входа. Интернет-технологии легко позволяют людям общаться с почти безграничной аудиторией в условиях относительной анонимности, быстро и эффективно преодолевая государственные границы. Интернет-технологии обладают многочисленными преимуществами, начиная с их уникальной пригодности для обмена информацией и идеями, что является одним из общепризнанных основополагающих прав человека[2]. Однако следует также признать, что те же технологии, которые способствуют такому общению, могут быть использованы в террористических целях. Использование Интернета в террористических целях как создает проблемы, так и открывает новые возможности в борьбе с терроризмом.

B. Методы, посредством которых Интернет используется в террористических целях

2. Для целей настоящей публикации в отношении классификации методов, посредством которых Интернет нередко используется для поощрения и поддержки террористических актов, был принят функциональный подход. На основе такого подхода были определены шесть иногда частично перекрывающих друг друга категорий: пропаганда (в том числе вербовка, радикализация и подстрекательство к терроризму); финансирование; обучение; планирование (в том числе с использованием секретной связи и открытых источников информации); исполнение; а также компьютерные атаки. Каждая из этих категорий более подробно рассматривается ниже.

1. Пропаганда

3. Одним из основных направлений использования Интернета террористами является пропагандистская деятельность. Обычно пропагандистские материалы имеют форму мультимедийных коммуникаций, содержащих идеологические или практические наставления, разъяснения, оправдания или рекламу террористической деятельности. К ним могут относиться виртуальные сообщения, презентации, журналы, теоретические работы, аудио- и видеофайлы, а также электронные игры, разрабатываемые террористическими организациями или их сторонниками. Тем не менее являющиеся террористической пропагандой материалы, в отличие от законной публичной защиты той или иной точки зрения, нередко носят характер субъективных оценок. Кроме того, распространение пропаганды само по себе, как правило, не является запрещенным видом деятельности. Одним из главных принципов международного права является защита основных прав человека, в число которых входит право на свободу выражения (обсуждение см. в разделе D главы I, ниже). Это гарантирует индивиду право, за

[2] См., например, Международный пакт о гражданских и политических правах (резолюция 2200 A (XXI) Генеральной Ассамблеи, приложение), пункт 2 статьи 19.

некоторыми немногочисленными исключениями, делиться своим мнением или распространять информацию, которая другим может представляться нежелательной. Одним из общепринятых исключений из этого права является запрет на распространение отдельных категорий материалов откровенно сексуального содержания, причем считается, что запрет на них введен в общественных интересах в целях защиты определенных уязвимых групп населения. Другие исключения, каждое из которых должно быть предусмотрено законом и необходимость которых должна быть доказана, могут включать сообщения, явно наносящие ущерб защите национальной безопасности, а также сообщения, имеющие целью и способные побудить людей к актам насилия в отношении отдельных лиц или определенных групп лиц[3].

4. Поощрение насилия является обычной темой связанной с терроризмом пропаганды. Широкая область влияния распространяемой через Интернет информации в геометрической прогрессии увеличивает аудиторию, на которую она может воздействовать. Кроме того, возможность непосредственного распространения контента через Интернет уменьшает зависимость от традиционных каналов связи, таких как новостные агентства, которые могут предпринять соответствующие шаги в целях самостоятельной оценки достоверности предоставленной информации либо отредактировать и опустить аспекты, считающиеся недопустимо провокационными. Интернет-пропаганда также может включать такой контент, как видеосюжеты о насильственных террористических актах или создаваемые террористическими организациями видеоигры, имитирующие акты терроризма и побуждающие пользователей участвовать в ролевой игре, выступая в роли виртуального террориста.

5. Пропаганда экстремистской риторики с призывами к насильственным действиям также является общей тенденцией для все более широкого круга интернет-платформ, предоставляющих услуги по размещению информационного наполнения, создаваемого пользователями. Материалы, которые прежде могли распространяться – лично или с помощью физических носителей, таких как компакт-диски (CD) и цифровые видеодиски (DVD), – среди относительно ограниченной аудитории, все чаще переносятся в Интернет. Такие материалы могут распространяться с использованием широкого спектра инструментальных средств, таких, соответственно, как специализированные веб-сайты, целевые виртуальные чат-группы и чат-форумы, онлайн-журналы, платформы социальных сетей типа Twitter и Facebook, а также популярные видео- и файлообменные веб-сайты типа YouTube и Rapidshare. Использование служб индексации, таких как поисковые системы Интернета, также упрощает процесс нахождения и извлечения информационного наполнения, связанного с терроризмом.

6. Основная угроза, которую несет с собой террористическая пропаганда, связана с тем, как она используется и в каких целях распространяется. Распространяемая через Интернет террористическая пропаганда охватывает ряд задач и аудиторий. Она может быть приспособлена для воздействия, в частности, на потенциальных или реальных сторонников или противников той или иной организации или общих экстремистских воззрений, на прямых или косвенных жертв террористических актов или на международное сообщество в целом либо какую-то его часть. Ориентированная на потенциальных или реальных сторонников пропаганда может быть направлена на вербовку, радикализацию и подстрекательство к терроризму путем рассылки сообщений с выражением чувств гордости, удовлетворения от успехов и преданности экстремистским целям. Она также может использоваться в качестве доказательства успешного проведения террористических актов для тех, кто обеспечивает соответствующую финансовую поддержку. Другие цели террористической пропаганды могут включать использование психологического манипулирования для подрыва веры отдельных лиц в некоторые коллективные социальные ценности или для распространения чувств повышенной тревоги, страха или паники среди населения или отдельных групп населения. Это может достигаться путем распространения дезинформации, слухов, угроз применения

[3] Там же, пункт 3 статьи 19.

насилия или изображений, связанных с вызывающими актами насилия. Целевая аудитория может включать как тех, кто непосредственно видит эти материалы, так и тех, кто окажется под воздействием потенциальной огласки, которую такие материалы приобретают. Что касается более широких кругов международной общественности, то здесь цель нередко заключается в том, чтобы распространить мысль о стремлении к достижению благородных политических целей[4].

a) Вербовка

7. Интернет может использоваться не только в качестве средства для публикации экстремистской риторики и видеоматериалов, но и как способ установления отношений с теми, кто наиболее склонен поддаваться на целенаправленную пропаганду, и поиска их поддержки. Террористические организации все чаще используют пропаганду, распространяемую через такие платформы, как защищенные паролем веб-сайты и чат-группы ограниченного доступа в Интернете, как средство тайной вербовки[5]. Совокупная аудитория Интернета обеспечивает террористическим организациям и их сторонникам глобальный резерв потенциальных новобранцев. Интернет-форумы ограниченного доступа становятся для новообращенных тем местом, где они могут узнать о террористических организациях и предложить им свою поддержку, а также приступить к непосредственным действиям, чтобы способствовать террористическим целям[6]. Использование технологических барьеров для доступа к платформам, на которых осуществляется вербовка, кроме того, усложняет процесс отслеживания сотрудниками разведки и правоохранительных органов связанной с терроризмом деятельности.

8. Террористическая пропаганда нередко специально рассчитана на то, чтобы быть притягательной для уязвимых и маргинализованных групп общества. В процессе вербовки и радикализации террористы, как правило, играют на присутствующих у человека ощущениях несправедливости, изоляции или унижения[7]. Пропаганда может также быть адаптирована таким образом, чтобы учитывать демографические факторы, например возраст или пол, а также социальные или экономические обстоятельства.

9. Интернет может служить особенно эффективным средством вербовки несовершеннолетних, которые составляют значительную часть пользователей. Распространяемые через Интернет в целях вербовки несовершеннолетних пропагандистские материалы могут принимать формы мультфильмов, популярных музыкальных видеозаписей или компьютерных игр. Тактика, применяемая на веб-сайтах, которые поддерживаются террористическими организациями или их сообщниками в целях вербовки несовершеннолетних, включает использование смеси мультфильмов и рассказов для детей с сообщениями, в которых поощряются и прославляются террористические акты, такие как миссии террористов-смертников. Аналогичным образом, некоторые террористические организации разрабатывают действующие в онлайновом режиме видеоигры, предназначенные для использования в качестве инструментов вербовки и обучения новичков. Такие игры могут служить средством пропаганды применения насилия в отношении государства или видных политических деятелей, предлагая награду за виртуальный успех, и могут выпускаться на разных языках в целях привлечения более широкого круга поклонников[8].

---

[4]Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C., United States Institute of Peace Press, 2006), pp. 37-38.

[5]Scott Gerwehr and Sarah Daly, "Al-Qaida: terrorist selection and recruitment", in *The McGraw-Hill Homeland Security Handbook*, David Kamien, ed. (New York, McGraw-Hill, 2006), p. 83.

[6]Dorothy E. Denning, "Terror's web: how the Internet is transforming terrorism", in *Handbook of Internet Crime*, Yvonne Jewkes and Majid Yar, eds. (Cullompton, United Kingdom, Willan Publishing, (2010)), pp. 194-213.

[7]European Commission, Expert Group on Violent Radicalisation, "Radicalisation processes leading to acts of terrorism" (2008). См. по адресу: www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf.

[8]Gabriel Weimann, "Online terrorists prey on the vulnerable", *YaleGlobal Online*, 5 March 2008. См. по адресу: http://yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable.

b) Подстрекательство

10. В то время как ведение пропагандистской деятельности само по себе обычно не запрещается, использование пропаганды террористами для подстрекательства к актам терроризма во многих государствах-членах считается противозаконным. В Интернете имеется множество материалов и возможностей для загрузки, редактирования и распространения информационного наполнения, которое может рассматриваться как незаконное прославление террористических актов или подстрекательство к их совершению. Следует отметить, однако, что ряд межправительственных организаций и правозащитных механизмов выражают сомнение в том, что понятие "прославление" терроризма является достаточно узким и точным и может служить основой для уголовных санкций, совместимых с требованиями закрепленного в статьях 15 и 19 Международного пакта о гражданских и политических правах[9, 10] принципа законности и допустимыми ограничениями права на свободу выражения.

11. Важно подчеркнуть различие между простой пропагандой и материалами, имеющими целью подстрекательство к актам терроризма. В ряде государств-членов, для того чтобы привлечь кого-либо к ответственности за подстрекательство к терроризму, требуется доказать наличие необходимого умысла и прямой причинно-следственной связи между предполагаемой пропагандой и реальным заговором или осуществлением террористического акта. Например, в своем выступлении на совещании группы экспертов один из французских экспертов отметил, что распространение учебных материалов по взрывчатым веществам не будет считаться нарушением французских законов, если в соответствующем сообщении не содержится информации, указывающей на то, что данный материал распространяется в поддержку осуществления террористических целей.

12. Как предусмотрено в пункте 3 статьи 19 Международного пакта о гражданских и политических правах, предупреждение и сдерживание подстрекательства к терроризму в интересах защиты национальной безопасности и общественного порядка являются законными основаниями для ограничения свободы выражения своего мнения. Эти основания также соответствуют положениям пункта 2 статьи 20 Пакта, требующим от государств запрещения всяких выступлений в пользу национальной, расовой или религиозной ненависти, представляющих собой подстрекательство к дискриминации, вражде или насилию. Однако, поскольку право на свободу выражения носит основополагающий характер, любые ограничения на осуществление данного права должны быть необходимы и пропорциональны существующей угрозе. Право на свободу выражения мнения также связано с другими важными правами, включая право на свободу мысли, совести и религии, убеждений и мнения[11].

c) Радикализация

13. Вербовка, радикализация и подстрекательство к терроризму могут рассматриваться как элементы в цепочке тесно связанных между собой явлений. Радикализация относится прежде всего к процессу идеологической обработки, который нередко сопутствует превращению завербованных неофитов в лиц, преисполненных решимости совершать насильственные действия на основе экстремистских идеологий. Процесс радикализации часто включает использование пропаганды, которая на протяжении длительного времени ведется либо посредством личного общения, либо через Интернет. Продолжительность и эффективность пропаганды и

[9] Резолюция 2200 A (XXI) Генеральной Ассамблеи, приложение.

[10] См. следующие доклады Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом: A/65/258 (пункт 46) и A/61/267 (пункт 7); см. также доклад Специального докладчика по вопросу о поощрении и защите прав на свободу мнений и их свободное выражение, добавление, касающееся десятой годовщины совместной декларации: десять основных задач в области свободы выражения мнений в следующем десятилетии (A/HRC/14/23/Add.2).

[11] Office of the United Nations High Commissioner for Human Rights, "Human rights, terrorism and counter-terrorism", Fact Sheet No. 32 (Geneva, 2008), Chap. III, sect. H.

других используемых средств убеждения варьируется в зависимости от конкретных обстоятельств и отношений.

2. Финансирование

14. Террористические организации и их сторонники также могут использовать Интернет для финансирования террористических актов. Методы, с помощью которых террористы используют Интернет для мобилизации и сбора средств и ресурсов, можно подразделить на четыре основные категории: прямые просьбы о пожертвованиях, электронная коммерция, использование действующих в Интернете платежных инструментов, а также посредничество благотворительных организаций. В случае прямых обращений речь идет об использовании веб-сайтов, чат-групп, массовых рассылок и целенаправленных сообщений в целях передачи просьб о пожертвованиях от сторонников. Веб-сайты также могут использоваться в качестве интернет-магазинов, предлагающих сторонникам книги, аудио- и видеозаписи и другие товары. Платежные средства, предоставляемые в Интернете через специализированные веб-сайты или коммуникационные платформы, позволяют легко осуществлять электронный перевод средств между сторонами. Переводы средств нередко производятся с помощью электронных банковских переводов, кредитных карт или иных платежных средств, доступных через такие сервисы, как PayPal или Skype.

15. Онлайновые платежные средства также могут использоваться мошенническим путем с помощью таких приемов, как хищение личных данных, кражи кредитных карт, мошенничество с использованием электронных средств коммуникации, биржевое мошенничество, преступления против интеллектуальной собственности и мошенничество на аукционах. Примером использования незаконных доходов для финансирования террористических актов может служить дело *Соединенное Королевство против Юниса Цули* (см. пункт 114, ниже). Прибыль от украденных кредитных карт была отмыта несколькими способами, включая перевод через электронную платежную систему e-gold ("электронное золото"), которая была использована для пересылки средств транзитом через ряд стран, прежде чем они попали в пункт своего назначения. Отмытые деньги использовались как для финансирования зарегистрированных Цули 180 веб-сайтов, на которых были размещены пропагандистские видеоматериалы движения "Аль-Каида", так и в целях приобретения снаряжения для террористической деятельности в ряде стран. Для незаконного получения порядка 1,6 млн. фунтов стерлингов на финансирование террористической деятельности были использованы около 1400 кредитных карт[12].

16. Финансовая поддержка, оказываемая, казалось бы, законным организациям, например благотворительным, также может быть перенаправлена на незаконные цели. Как известно, некоторые террористические организации создают подставные корпорации, маскируемые под благотворительные предприятия, чтобы ходатайствовать о предоставлении средств по электронным каналам. Эти организации могут утверждать, что поддерживают гуманитарные цели, тогда как на самом деле пожертвования используются для финансирования террористических актов. Примерами якобы благотворительных организаций, используемых в террористических целях, являются носящие безобидные названия "Беневоленс интернешнл фаундейшн", "Глоубал рилиф фаундейшн" и Фонд Палестины в целях оказания помощи и развития – все они пользовались полученными мошенническим путем средствами для финансирования террористических организаций на Ближнем Востоке. Террористы также могут внедряться в филиалы благотворительных организаций, которые используются ими в качестве прикрытия для распространения идеологии террористических организаций или для оказания материальной поддержки группам боевиков[13].

[12] Письменный материал, представленный экспертом из Соединенного Королевства.

[13] Maura Conway, "Terrorist 'use' of the Internet and fighting back", *Information & Security*, vol. 19 (2006), pp. 12-14.

3. Подготовка террористов

17. В последние годы террористические организации все чаще прибегают к использованию Интернета в качестве альтернативной базы для подготовки террористов. Все более широкий спектр средств информации предоставляет платформы для распространения практических руководств в виде интерактивных учебных пособий, аудио- и видеоклипов, информационных сообщений и рекомендаций. На этих интернет-платформах также публикуются подробные инструкции, часто в легкодоступном мультимедийном формате и на нескольких языках, по вопросам о том, например, как вступить в террористические организации, как изготовить взрывчатые боеприпасы, огнестрельное и другие виды оружия или опасные материалы и как планировать и осуществлять террористические акты. Эти платформы выступают в качестве виртуальной учебной базы. Кроме того, они используются, в частности, для обмена специальными методами, приемами или оперативными знаниями в целях совершения террористических актов.

18. Например, журнал "Inspire" является интернет-изданием, предположительно выпускаемым "Аль-Каидой" на Аравийском полуострове с заявленной целью дать мусульманам возможность готовиться к участию в джихаде у себя на дому. В нем публикуется большое количество идеологических материалов, направленных на поощрение терроризма, в том числе заявления, приписываемые Усаме бен Ладену, шейху Айману аз-Завахири и другим известным деятелям "Аль-Каиды". В осенний выпуск 2010 года были включены практические учебные материалы о том, как приспособить полноприводный автомобиль для проведения акта нападения на представителей общественности и как боевик-одиночка может осуществить неизбирательное нападение, стреляя из огнестрельного оружия с высокого здания. В этом издании даже имелось предложение относительно того, какой город следует избрать для такой атаки, чтобы повысить шансы убить членов правительства[14].

19. В имеющихся в Интернете учебных материалах предлагаются инструменты для содействия контрразведывательной деятельности и неавторизованному доступу к компьютерным данным, а также для повышения уровня защищенности противозаконных коммуникаций и деятельности в Сети путем использования доступных средств шифрования и методов анонимизации. Интерактивный характер интернет-платформ помогает создать чувство общности между людьми, живущими в разных географических регионах и имеющими различное происхождение, способствуя созданию сетей для обмена материалами учебного и тактического характера.

4. Планирование

20. Многие работники системы уголовного правосудия указывают, что почти каждое из рассматриваемых в судах дел против террористов связано с использованием интернет-технологий. В частности, при планировании террористических актов обычно имеет место дистанционный обмен сообщениями между несколькими сторонами. Недавно слушавшееся во Франции дело *Государственный обвинитель против Ишора*[15] показывает, каким образом различные виды интернет-технологий могут использоваться в целях содействия подготовке террористических актов, в том числе посредством обеспечения связи как внутри организаций, выступающих за насильственный экстремизм, так и между ними, включая связь через границы.

[14] Письменный материал, представленный экспертом из Соединенного Королевства.

[15] Судебное решение от 4 мая 2012 года, дело № 0926639036, Суд большой инстанции города Парижа (14-я палата/2), Париж.

Государственный обвинитель против Ишора

В мае 2012 года французский суд приговорил Адлена Ишора, гражданина Франции алжирского происхождения, к пяти годам лишения свободы за участие в преступном сговоре в целях подготовки террористического акта (по статье 421-1 и далее Уголовного кодекса Франции) в связи с действиями, совершенными во Франции в 2008 и 2009 годах.

Расследование причастности Ишора, являющегося физиком-ядерщиком, было начато в начале 2008 года в связи с отправленным на сайт президента Французской Республики электронным сообщением джихадистского содержания, которое, как было прослежено, исходило от одного из членов "Аль-Каиды" в странах исламского Магриба (АКИМ).

Изданное в январе 2009 года распоряжение об охране позволило органам власти выявить обмены сообщениями по электронной почте между этим членом АКИМ и, в частности, Глобальным исламским информационным фронтом (ГИИФ) и центром "Рафидаин" (Rafidayin Center) – веб-сайтом с заявленной целью размещать и распространять документы, аудио- и видеозаписи "Аль-Каиды", заявления ее полевых командиров и террористов-смертников, а также материалы других экстремистских исламских групп. Эта электронная переписка кодировалась с помощью специального программного обеспечения "Асрар-эль-моджахедин", или "Секреты моджахедов", которое включает 256-битовое шифрование, переменные криптографические ключи секретных шифров, 2048-битовые криптографические ключи шифрования в рамках СКО и средства оперативной пересылки шифрованных сообщений через чат-форумы.

На суде были представлены десятки расшифрованных сообщений из электронной почты. Обвинение утверждало, как указывает содержание этих электронных писем, что Ишор активно выполнял среди прочего следующие действия в поддержку джихадистской сети, в частности от имени центра "Рафидаин":

- переводил, шифровал, сжимал и защищал паролями проджихадистские материалы, в том числе документы и видео, которые он затем пересылал и распространял через Интернет;
- распространял криптографическое программное обеспечение "Секреты моджахедов" в целях содействия скрытому обмену сообщениями через Интернет;
- вступил в сговор с одним из членов АКИМ в целях организации и координации проджихадистской деятельности, включая в числе прочего предоставление финансовой поддержки делу джихада, распространение проджихадистской информации и содействие созданию оперативных групп в Европе, и в частности во Франции, для возможной подготовки террористических актов;
- выступал в качестве модератора на проджихадистском веб-сайте "Рибат";
- предпринял конкретные шаги для оказания финансовой поддержки АКИМ, в том числе пытаясь использовать PayPal и другие виртуальные платежные системы.

На суде обвинение утверждало, что эти сообщения являются доказательством того, что Ишор полностью сознавал, что имел дело с членом АКИМ и что он сознательно и добровольно выступал в качестве посредника между джихадистскими боевиками и ГИИФ. По завершении судебного разбирательства суд решил, что "Ишор оказывал... логистическую и медийную поддержку этой террористической структуре, для которой "джихад в средствах массовой информации" имеет решающее значение".

Кроме того, суд постановил, что "Адлен Ишор, согласившись на создание связанного с АКИМ оперативного подразделения в Европе, может быть даже во Франции, и намечая цели или категории целей для нанесения ударов, участвовал в деятельности группы [АКИМ], специально созданной для подготовки террористических актов".

Поэтому суд пришел к заключению, что имеется достаточно доказательств, чтобы продемонстрировать, как того требует Уголовный кодекс Франции, что Ишор оказывал не только интеллектуальную, но и прямую логистическую поддержку в осуществлении явно установленного террористического плана. Решение суда может быть обжаловано.

Источники: Решение Суда большой инстанции города Парижа от 4 мая 2012 года; и Tung, Liam, *Jihadists get world-class encryption kit* (29 January 2008), см. по адресу: www.zdnet.com.au/jihadists-get-world-class-encryption-kit-339285480.htm.

21. Через Интернет также могут предприниматься шаги для определения потенциальной цели нападения и наиболее эффективных средств достижения цели террористического акта. Эти подготовительные шаги могут варьироваться от получения инструкций в отношении рекомендуемых методов нападения до сбора информации о предполагаемой цели из открытых и иных источников. Открываемые в Интернете возможности для преодоления расстояний и границ и огромное количество имеющейся в киберпространстве общедоступной информации делают Интернет ключевым инструментом планирования террористических актов.

a) Секретная связь в процессе подготовки

22. Самой главной функцией Интернета является обеспечение удобства передачи информации. Террористы становятся все более искушенными в использовании коммуникационных технологий в целях обмена анонимными сообщениями, связанными с планированием террористических актов. В качестве электронного, или виртуального, "тайника" для доставки сообщений террористы могут использовать обычные учетные записи абонентов электронной почты в Интернете. Речь идет о создании черновика сообщения, который остается неотправленным и, соответственно, оставляет минимум электронных следов, но может быть доступен с любого интернет-терминала в любой точке мира для ряда лиц, обладающих соответствующим паролем.

23. Также существует множество более сложных технологий, которые затрудняют распознавание отправителя, получателя или содержания интернет-сообщений. В Интернете легкодоступны для скачивания средства шифрования и программное обеспечение для анонимизации трафика. Эти инструментальные средства способны, в частности, замаскировать уникальный адрес по протоколу Интернет (IP), идентифицирующий каждое используемое для доступа в Интернет устройство и его местоположение, перенаправить интернет-сообщения через один или несколько серверов в юрисдикции с более низкими уровнями правоприменения в отношении террористической деятельности и/или зашифровать данные трафика, относящиеся к посещаемым веб-сайтам. Также может использоваться стеганография – сокрытие сообщений в графических изображениях.

b) Общедоступная информация

24. Организации и частные лица нередко публикуют в Интернете значительные объемы информации. В случае организаций это отчасти может быть вызвано желанием создать рекламу своей деятельности и оптимизировать свое взаимодействие с общественностью. Через поисковые системы в Интернете, способные каталогизировать и извлекать не имеющую надлежащей защиты информацию с миллионов веб-сайтов, можно также получить доступ к некоторому количеству секретной информации, которая может использоваться террористами в противозаконных целях. Кроме того, интерактивный доступ к подробной логистической информации, такой как производимые в режиме реального времени съемки замкнутых телевизионных сетей, а также такие прикладные программы, как Google Earth, предназначенная для физических лиц и в основном используемая ими в законных целях, могут использоваться

в неблаговидных целях теми, кто стремится воспользоваться преимуществами свободного доступа к получаемым с помощью ИСЗ изображениям, картам и информации о местности и сооружениях в высоком разрешении для ведения рекогносцировки потенциальных целей с удаленных компьютерных терминалов.

25. В частности, в эпоху популярных социальных медиасетей, таких как Facebook, Twitter, YouTube, Flickr и блогерские платформы, частные лица также публикуют в Интернете, добровольно или по неосмотрительности, беспрецедентное количество конфиденциальной информации. В то время как намерение лиц, распространяющих такие материалы, может состоять в том, чтобы донести до своей аудитории новости или иные свежие сведения в информационных или социальных целях, часть этой информации может быть незаконно присвоена и использована в интересах преступной деятельности.

5. Исполнение

26. Элементы описанных выше категорий могут применяться при использовании Интернета для осуществления террористических актов. Например, явные угрозы насилием, в том числе связанным с применением оружия, могут распространяться через Интернет, чтобы посеять тревогу, страх или панику среди населения или каких-либо групп населения. В ряде государств-членов факт распространения таких угроз, даже если они не исполняются, может быть признан преступлением. Например, в Китае фабрикация угрозы и/или распространение угрозы, в отношении которой известно, что ее содержание связано с использованием бомб, либо биологических, химических или радиоактивных материалов, либо иных видов оружия, если данное деяние совершается с намерением "серьезно подорвать общественный порядок", считается в соответствии с национальным законодательством преступлением[16]. В качестве средства установления контактов с потенциальными жертвами или для координации фактического исполнения террористических актов также могут использоваться передаваемые через Интернет сообщения. Например, Интернет широко использовался в целях координации действий участников терактов 11 сентября 2001 года в Соединенных Штатах.

27. Использование Интернета в целях содействия проведению террористических актов может, в частности, обеспечить логистические преимущества, снизить вероятность обнаружения или затруднить идентификацию ответственных за преступление сторон. Деятельность в Интернете может также упростить приобретение материалов, необходимых для осуществления теракта. Пользуясь средствами электронной торговли, террористы могут приобретать отдельные компоненты или услуги, необходимые для совершения террористических актов. А для финансирования таких покупок могут применяться неправомерно присвоенные кредитные карты или другие формы неправомерного использования систем электронных платежей.

6. Кибератаки

28. Термин "кибератака" обычно означает преднамеренное использование компьютерных сетей в качестве средства для нанесения удара. Такие атаки, как правило, имеют целью нарушить нормальное функционирование таких объектов нападения, как компьютерные системы, серверы или базовая инфраструктура, с помощью "хакинга", изощренных способов создания стойких угроз, компьютерных вирусов, вредоносных программ[17],

[16] Письменный материал, представленный экспертом из Китая.

[17] Согласно подпункту *n)* раздела 1 подготовленного Международным союзом электросвязи Инструментария для разработки законодательства по киберпреступности, "вредоносную программу" можно определить как программу, вставляемую, обычно скрытно, в компьютерные программы и системы в целях нарушения секретности, целостности и доступности компьютерной программы, информации или системы.

"флудинга"[18] или других средств несанкционированного либо злонамеренного доступа. Кибератаки могут иметь характерные черты террористического акта, в частности, их главной мотивировкой является стремление посеять страх, чтобы содействовать достижению политических или социальных целей. В качестве примера можно привести случай кибератаки в Израиле в январе 2012 года, когда объектом нападения стал ряд имеющих символическое значение израильских веб-сайтов, таких как сайты Тель-Авивской фондовой биржи и национальной авиакомпании, результатом чего было несанкционированное раскрытие данных о кредитных картах и банковских реквизитах тысяч израильских граждан[19]. Хотя в последние годы угрозе кибератак со стороны террористов уделяется значительное внимание, данная тема выходит за рамки настоящей публикации и сама по себе предметом анализа являться не будет.

C. Использование Интернета в целях противодействия террористической деятельности

29. Хотя террористами разработан ряд способов использования Интернета для содействия достижению противозаконных целей, само использование ими Интернета также открывает возможности для сбора разведывательной информации и проведения иных мероприятий, направленных на предотвращение и пресечение террористических актов, а также для сбора доказательств в целях уголовного преследования за совершение таких актов. Значительный объем знаний о функционировании, видах деятельности, а иной раз и об объектах нападения террористических организаций удается извлечь из сообщений на веб-сайтах, в чатах и других интернет-ресурсах. Кроме того, чем шире Интернет используется в террористических целях, тем более доступными, соответственно, становятся электронные данные, которые можно подвергать обобщению и анализу в целях борьбы с терроризмом. Правоохранительные, разведывательные и другие органы разрабатывают все более совершенные инструменты для активного предотвращения, обнаружения и сдерживания террористической деятельности, связанной с использованием Интернета. Все шире применяются также традиционные методы следствия, такие как выделение специализированных переводческих ресурсов для своевременного выявления потенциальных террористических угроз.

30. Онлайновые обсуждения дают возможность выражать противоположные точки зрения или вести конструктивные дискуссии, которые способны отвратить потенциальных сторонников террористов. Контртеррористические материалы, твердо опирающиеся на факты, можно доносить до целевой аудитории через дискуссионные интернет-форумы, а также в виде изображений и видео. Эффективные сообщения, помимо прочего, могут содержать выражение сочувственного отношения к глубинным проблемам, способствующим радикализации, таким как политические и социальные условия, и предлагать альтернативы насильственным методам достижения желаемых результатов[20]. Кроме того, в целях охвата широкой, разнообразной в географическом плане аудитории стратегически важные сообщения, содержащие воспитательно-просветительские материалы для развенчания террористической пропаганды, могут распространяться через Интернет на многих языках.

[18] "Флудинг" означает избрание в качестве объекта нападения центральных аутентификационных серверов той или иной организации, на которые одновременно направляется множество запросов об аутентификации в целях перегрузить эти серверы, результатом чего становится распределенный отказ в обслуживании.

[19] См. Isabel Kershner, "Cyberattack exposes 20,000 Israeli credit card numbers and details about users", *New York Times*, 6 January 2012; а также "2 Israeli web sites crippled as cyberwar escalates", *New York Times*, 16 January 2012.

[20] Рабочая группа по противодействию использованию Интернета в террористических целях, учрежденная Целевой группой по осуществлению контртеррористических мероприятий, "Резюме Конференции и последующие рекомендации" Конференции по вопросам использования Интернета для противодействия экстремистским призывам к насилию", состоявшейся в Эр-Рияде 24–26 января 2011 года. См. по адресу: www.un.org/en/terrorism/ctitf/pdfs/ctitf_riyadh_conference_summary_recommendations.pdf.

31. Базирующийся в Соединенных Штатах Центр стратегической контртеррористической информации является одним из примеров предпринимаемых в последнее время межучрежденческих инициатив, направленных на снижение уровней радикализации и экстремистского насилия путем своевременного выявления экстремистской пропаганды, в том числе в Интернете, и быстрого реагирования на нее посредством целенаправленного распространения контрпропагандистских материалов с использованием широкого спектра коммуникационных технологий, включая цифровые инструментальные средства[21]. Например, как стало известно, в мае 2012 года Центр, в ответ на размещенный на различных сайтах "Аль-Каиды" на Аравийском полуострове рекламный баннер с призывами к экстремистскому насилию, в течение 48 часов разместил на тех же веб-сайтах антирекламные объявления, представлявшие собой видоизмененную версию экстремистского сообщения и информировавшие о том, что жертвами деятельности данной террористической организации являются граждане Йемена. Проведение данной контрпропагандистской кампании было связано с сотрудничеством между Государственным департаментом Соединенных Штатов, разведывательным сообществом и военными. Центр также использует для распространения контртеррористических материалов такие медийные платформы, как Facebook и YouTube[22, 23].

D. Соображения с позиций верховенства права

32. Неотъемлемой составляющей борьбы с терроризмом являются уважение прав человека и верховенство права. Вопросам соблюдения международных норм в области прав человека необходимо уделять должное внимание на всех этапах реализации инициатив по борьбе с терроризмом, начиная с профилактического сбора разведывательных данных и до обеспечения соблюдения надлежащей правовой процедуры в процессе судебного преследования подозреваемых. Для этого требуется выработать национальное антитеррористическое законодательство и практику, направленные на поощрение и защиту основных прав человека и принципа верховенства права[24].

33. Государства имеют право и обязаны принимать эффективные меры в целях противодействия разрушительным последствиям терроризма для прав человека, в частности прав на жизнь, свободу и физическую неприкосновенность личности и на территориальную целостность и безопасность государств. Эффективные меры по борьбе с терроризмом и защита прав человека являются взаимодополняющими и взаимоподкрепляющими целями, и добиваться их осуществления необходимо одновременно[25]. Связанные с использованием Интернета инициативы в области борьбы с терроризмом могут воздействовать на осуществление ряда прав человека, включая права на свободу слова, свободу ассоциации, неприкосновенность частной жизни и справедливое судебное разбирательство. В то время как всесторонний анализ вопросов прав человека выходит за рамки настоящей публикации, важно обратить внимание на ряд ключевых областей, требующих рассмотрения.

34. Как отмечалось в подпункте *b)* пункта 1 раздела B, выше, запрещение подстрекательства к терроризму может быть связано с ограничениями свободы выражения.

---

[21] Executive Order 13584 of 9 September 2011, "Developing an Integrated Strategic Counterterrorism Communications Initiative and Establishing a Temporary Organization to Support Certain Government-wide Communications Activities Directed Abroad", *Federal Register*, vol. 76, No. 179, 15 September 2011.

[22] "United States State Department fights al-Qaeda in cyberspace", *Al Jazeera* (25 May 2012). См. по адресу: http://blogs.aljazeera.com/americas/2012/05/25/us-state-department-fights-al-qaeda-cyberspace.

[23] "U.S. uses Yemeni web sites to counter al-Qaeda propaganda", *The Washington Post* (24 May 2012). См. по адресу: www.washingtonpost.com/world/national-security/us-hacks-web-sites-of-al-qaeda-affiliate-in-yemen/2012/05/23/gJQAGnOxlU_story.html.

[24] Управление Верховного комиссара Организации Объединенных Наций по правам человека, "Изложение фактов" № 32, глава III, раздел H.

[25] Там же, глава I, раздел C.

Свобода выражения не является абсолютным правом. Если такая свобода используется для подстрекательства к дискриминации, враждебности или насилию, она может быть ограничена при условии соблюдения жестких критериев законности, необходимости, пропорциональности и недопущения дискриминации.

В случаях прославления терроризма или подстрекательства к нему основная сложность заключается в том, как определить границы допустимого, поскольку в этом отношении страны существенно различаются в зависимости от особенностей их культурной и правовой истории[26]. Аналогичным образом, условный характер также носит право на свободу ассоциации, которое может подвергаться строго определенным ограничениям и отступлениям.

35. Противодействие использованию Интернета террористами может включать установление наблюдения за подозреваемыми и сбором относящейся к ним информации. Должное внимание при этом следует уделять защите людей от произвольного или незаконного нарушения их права на неприкосновенность частной жизни[27], которое включает право на тайну информации о личности человека, а также о его или ее личной жизни. Во внутригосударственном законодательстве должны быть достаточно подробно освещены вопросы, касающиеся, в том числе, конкретных обстоятельств, в которых такое нарушение может быть допустимо. Необходимо также ввести соответствующие гарантии в целях предотвращения злоупотребления средствами негласного надзора. Кроме того, любые собранные персональные данные должны быть надлежащим образом защищены, чтобы исключить незаконный или произвольный доступ к ним, а также раскрытие или использование[28].

36. Решающее значение для обеспечения эффективности контртеррористических мер и применения их с учетом принципа верховенства права имеют гарантии прав на соблюдение предусмотренных законом процессуальных норм. Средства защиты прав человека любых лиц, обвиняемых в совершении уголовных преступлений, в том числе преступлений, связанных с терроризмом, включают право на презумпцию невиновности, право на слушание дела с соблюдением надлежащих гарантий и в разумный срок компетентным, независимым и беспристрастным судом, а также право на пересмотр обвинительного приговора и назначенного наказания вышестоящей судебной инстанцией, учитывающей те же стандарты[29].

37. Ознакомиться с более подробным анализом затрагиваемых в настоящем разделе вопросов и с другими соответствующими соображениями можно, например, в информационном бюллетене "Изложение фактов" № 32 Управления Верховного комиссара Организации Объединенных Наций по правам человека "Права человека, терроризм и борьба с терроризмом", докладе Верховного комиссара Организации Объединенных Наций по правам человека о защите прав человека и основных свобод в условиях борьбы с терроризмом (A/HRC/16/50), а также в следующих докладах Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом: "Десять элементов наилучшей практики в области борьбы с терроризмом" (A/HRC/16/51) и "Подборка оптимальных практических методов, применяемых в отношении законодательной и институциональной основы и мер, которые обеспечивают соблюдение прав человека специальными службами в условиях борьбы с терроризмом, в том числе касающихся надзора за их деятельностью" (A/HRC/14/46).

[26] Организация по безопасности и сотрудничеству в Европе, Бюро по демократическим институтам и правам человека, "Соблюдение прав человека в ходе борьбы с подстрекательством к терроризму и связанными с ним правонарушениями", справочный документ, подготовленный к состоявшемуся 19–20 октября 2006 года в Вене семинару-практикуму экспертов по теме "Предупреждение терроризма: борьба с подстрекательством к совершению террористических актов и связанной с терроризмом деятельностью", разделы 3 и 4.

[27] См. Международный пакт о гражданских и политических правах, статья 17.

[28] Права человека, терроризм и борьба с терроризмом, глава III, раздел J.

[29] Там же, глава III, раздел F.

II. Международный контекст

A. Введение

38. Использование Интернета террористами – это транснациональная проблема, для решения которой требуются согласованные ответные меры трансграничного характера с участием различных национальных систем уголовного правосудия. Центральная роль в связи с этим принадлежит Организации Объединенных Наций, которая содействует проведению соответствующих обсуждений и обмену передовым опытом между государствами-членами, а также достижению консенсуса в отношении общих подходов к вопросам борьбы с такими явлениями, как использование Интернета в террористических целях.

39. Применимая международно-правовая база по борьбе с терроризмом содержится в различных источниках, включая резолюции Генеральной Ассамблеи и Совета Безопасности, договоры, судебную практику и международное обычное право. Резолюции Совета Безопасности могут налагать на государства-члены юридически связывающие обязательства или являться принадлежащими к сфере "мягкого права" источниками политических обязательств или новых международно-правовых норм. Резолюции Совета, принимаемые на основании главы VII Устава Организации Объединенных Наций, являются обязательными для всех государств-членов. Генеральная Ассамблея также приняла ряд резолюций о борьбе с терроризмом, которые служат полезными источниками "мягкого права" и имеют большое политическое значение, хотя они не имеют юридически обязательной силы[30].

40. Юридические обязательства также налагаются на государства в соответствии с двусторонними и многосторонними документами по борьбе с терроризмом. "Универсальными" правовыми документами считаются соглашения, открытые для ратификации или присоединения к ним всех государств – членов Организации Объединенных Наций. В отличие от них, соглашения, промульгируемые региональными или иными межгосударственными объединениями, могут быть открытыми для ограниченной группы потенциальных подписантов; обязательства, основанные на договорах такого рода, являются юридически связывающими только для тех государств, которые решили стать участниками этих соглашений.

41. Обязанность привлекать виновных в совершении актов терроризма к судебной ответственности ложится прежде всего на внутригосударственные органы власти, поскольку международные суды, как правило, не обладают юрисдикцией в отношении таких актов[31]. Резолюции Организации Объединенных Наций, универсальные правовые документы, региональные соглашения и типовые законы по борьбе с терроризмом играют ключевую роль в установлении общих стандартов, признаваемых в ряде юрисдикций.

---

[30] См.: Управление Организации Объединенных Наций по наркотикам и преступности, Часто задаваемые вопросы о международно-правовых аспектах борьбы с терроризмом (2009 год). См. по адресу: www.unodc.org/documents/terrorism/Publications/FAQ/English.pdf.

[31] Специальный трибунал по Ливану, учрежденный в соответствии с резолюцией 1757 (2007) Совета Безопасности, в настоящее время является единственным международным судом с ограниченной юрисдикцией в отношении преступлений, связанных с терроризмом.

B. Резолюции Организации Объединенных Наций по борьбе с терроризмом

42. Глобальная контртеррористическая стратегия Организации Объединенных Наций[32] была единогласно принята Генеральной Ассамблеей в 2006 году и стала важной вехой в области многосторонних инициатив по борьбе с терроризмом. Согласно этой Стратегии государства-члены постановили, в частности:

a) последовательно, безоговорочно и решительно осудить терроризм во всех его формах и проявлениях, кем бы, где бы и с какой бы целью он ни осуществлялся, поскольку он является одной из самых серьезных угроз международному миру и безопасности;

b) принять незамедлительные меры по предотвращению терроризма и борьбе с ним во всех его формах и проявлениях;

c) признать, что международное сотрудничество и любые меры, которые [мы] примем для предотвращения терроризма и борьбы с ним, должны обеспечивать соблюдение всех [наших] обязательств по международному праву, в том числе по Уставу Организации Объединенных Наций и соответствующим международным конвенциям и протоколам, в частности норм в области прав человека, беженского права и международного гуманитарного права;

d) сотрудничать с Организацией Объединенных Наций при должном соблюдении принципов конфиденциальности, уважения прав человека и других обязательств, налагаемых нормами международного права, для изучения путей и средств: "*a) координации усилий, предпринимаемых на международном и региональном уровнях в целях борьбы с терроризмом во всех его формах и проявлениях в сети Интернет; b) использования сети Интернет в качестве инструмента борьбы с распространением терроризма, признавая при этом, что государствам может потребоваться помощь в этих вопросах*" [курсив наш].

43. В ряде принятых в последние годы резолюций Совета Безопасности содержится призыв к государствам всецело сотрудничать в борьбе с терроризмом во всех его формах. В частности, резолюции 1373 (2001) и 1566 (2004), принятые на основании главы VII Устава Организации Объединенных Наций, требуют от всех государств-членов принятия законодательных и иных мер, направленных на борьбу с терроризмом, в том числе путем расширения сотрудничества с другими правительствами в вопросах проведения расследований, обнаружения, ареста, выдачи и уголовного преследования лиц, причастных к совершению террористических актов, а также содержат призыв к государствам выполнять положения международных конвенций и протоколов, касающихся терроризма.

44. Еще одной ключевой резолюцией Совета Безопасности, касающейся террористической деятельности, которая может осуществляться с использованием Интернета, является резолюция 1624 (2005), в которой рассматриваются вопросы подстрекательства к совершению террористических актов и их прославления. В четвертом пункте ее преамбулы Совет осуждает "самым решительным образом подстрекательство к террористическим актам" и отвергает "попытки оправдания или прославления (апологии) террористических актов, которые могут побудить к совершению новых террористических актов". В пункте 1 Совет призывает все государства принять такие меры, которые могут быть необходимы и уместны и будут соответствовать их обязательствам по международному праву, чтобы законодательно запретить подстрекательство к совершению террористического акта или актов.

[32] Резолюция A/60/288 Генеральной Ассамблеи.

45. В последних докладах и резолюциях Организации Объединенных Наций конкретно признается важность противодействия использованию Интернета террористами в качестве одной из основных частей всеобъемлющей стратегии борьбы с терроризмом. В своем докладе Генеральной Ассамблее 2006 года под названием "Единство в борьбе с терроризмом: рекомендации по глобальной контртеррористической стратегии"[33] Генеральный секретарь прямо заявил: "Террористам необходима возможность получать и переводить финансовые средства, приобретать оружие, вербовать и готовить кадры и поддерживать связь, в частности через Интернет"[34]. Далее Генеральный секретарь указал, что Интернет быстро становится все более активным каналом вербовки террористов и распространения ими информации и пропаганды, чему необходимо противопоставить скоординированные действия государств-членов, осуществляемые на основе соблюдения прав человека и в соответствии с другими обязательствами по международному праву[35].

46. В своей резолюции 1963 (2010) Совет Безопасности выразил "озабоченность по поводу того, что в глобализованном обществе террористы все шире используют новые информационно-коммуникационные технологии, в частности Интернет, для целей вербовки и подстрекательства, а также для финансирования, планирования и подготовки своих акций". Совет также признал важность совместных действий государств-членов в целях недопущения использования террористами технологий, средств коммуникации и ресурсов.

C. Универсальные правовые документы по вопросам борьбы с терроризмом

47. С 1963 года международное сообщество под эгидой Организации Объединенных Наций и ее специализированных учреждений, в частности Международной организации гражданской авиации и Международной морской организации, а также Международного агентства по атомной энергии, ведет разработку универсальных правовых документов, направленных на предотвращение террористических актов. Универсальные документы по борьбе с терроризмом являются существенным элементом глобального режима борьбы с терроризмом и важной основой для международного сотрудничества в борьбе с терроризмом. Эти универсальные правовые документы охватывают деяния начиная от угона самолетов и до ядерного терроризма, совершаемые отдельными лицами и группами лиц[36], и требуют от принявших их государств установления уголовной ответственности за совершение наиболее предвидимых террористических актов в областях, на которые распространяется действие соответствующих конвенций. Тем не менее эти универсальные правовые документы являются юридически обязательными только для подписавших их государств[37], которые также несут ответственность за обеспечение применения их положений в рамках своих внутригосударственных систем уголовного правосудия.

48. В результате того что после принятия резолюции 1373 (2001) Совета Безопасности, в которой Совет призвал государства-члены стать участниками универсальных международно-правовых документов по борьбе с терроризмом, вопросам противодействия терроризму

[33] A/60/825.

[34] Там же, пункт 38.

[35] Там же, пункты 58 и 60.

[36] В число других охваченных террористических актов входят: акты авиационного саботажа, акты насилия в аэропортах, акты, направленные против безопасности морского судоходства, акты, направленные против безопасности стационарных платформ, расположенных на континентальном шельфе, преступления против лиц, пользующихся международной защитой (например, похищение дипломатов), акты, связанные с незаконным захватом ядерного материала и владением им, акты захвата заложников, акты бомбового терроризма и акты, связанные с финансированием совершения террористических актов и деятельности террористических организаций.

[37] Текущее состояние ратификации этих универсальных правовых документов см. по адресу: www.unodc.org/tldb/universal_instruments_NEW.html.

уделяется повышенное внимание, темпы присоединения государств к этим документам стали значительно выше. По состоянию на июнь 2011 года две трети государств-членов либо ратифицировали по меньшей мере 10 из 16 универсальных документов по борьбе с терроризмом, либо присоединились к ним[38].

49. В настоящее время всеобъемлющего договора Организации Объединенных Наций по борьбе с терроризмом, который был бы применим к исчерпывающему перечню проявлений терроризма, не существует. Также международное сообщество до сих пор не пришло к соглашению об обязательном в международном масштабе определении термина "терроризм"[39], главным образом из-за сложности выработки общеприемлемой правовой классификации актов насилия, совершаемых государствами, вооруженными группами, такими как движения за освобождение или самоопределение, или отдельными лицами.

50. С 2000 года государства-члены ведут переговоры в целях заключения всеобъемлющей конвенции о борьбе с терроризмом, в которую в конечном счете будет включено определение терроризма. Однако трудности в достижении консенсуса в отношении единого, признаваемого во всем мире определения того, что следует считать терроризмом, привели к тому, что некоторого прогресса удалось добиться в рамках уже существующих универсальных правовых документов, разработка которых велась по отраслевым направлениям. В этих документах акцент делается на криминализации конкретных "террористических актов", но не дается определения более широкого понятия терроризма.

51. В универсальных документах террористические преступления не квалифицируются как преступления по международному праву. Вместо этого они создают для государств – участников этих соглашений обязательство криминализовать указанное противоправное поведение в рамках своего внутреннего законодательства, осуществлять юрисдикцию в отношении правонарушителей в соответствии с установленными условиями и создать международные механизмы сотрудничества, позволяющие государствам-участникам либо привлекать к уголовной ответственности предполагаемых преступников, либо производить их выдачу. До успешного завершения текущих переговоров о выработке универсального определения или заключении всеобъемлющей конвенции, касающейся терроризма, в интересах содействия международному сотрудничеству основой для разработки общих стандартов противодействия использованию Интернета в террористических целях должны служить двусторонние и многосторонние соглашения.

52. Универсальной конвенции, специально направленной на предотвращение и пресечение использования Интернета террористами, пока не существует. В декабре 2010 года Генеральная Ассамблея приняла резолюцию 65/230, в которой она, в частности, одобрила Салвадорскую декларацию о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире[40] и просила Комиссию по предупреждению преступности и уголовному правосудию учредить, в соответствии с Салвадорской декларацией, межправительственную группу экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора,

[38] См. www.un.org/en/sc/ctc/laws.html.

[39] Стоит отметить, однако, что в недавнем решении Специального трибунала по Ливану было признано, что имеется достаточно доказательств, свидетельствующих о существовании определения преступления "терроризм", согласно нормам международного обычного права. См. Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, Case No. STL-11-01/I, Special Tribunal for Lebanon (16 February 2011); см. по адресу: http://www.stl-tsl.org/en/the-cases/stl-11-01/rule-176bis/filings/orders-and-decisions/appeals-chamber/f0010.

[40] Принята на двенадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, состоявшемся в Салвадоре, Бразилия, 12–19 апреля 2010 года, на котором среди прочего обсуждался вопрос о том, что государствам-членам необходимо продумать способы борьбы с новыми формами преступности, такими как киберпреступность.

включая обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве. Результаты этого исследования, которое было начато ЮНОДК в феврале 2012 года, будут способствовать оценке последствий использования вновь возникающих информационных технологий для содействия преступной деятельности, в том числе в отношении отдельных форм использования Интернета террористами, таких как преступления, связанные с подстрекательством к совершению террористических актов и финансированием терроризма с использованием компьютеров.

D. Международное право в области прав человека

53. Обязательства по соблюдению прав человека составляют неотъемлемую часть международно-правовой базы борьбы с терроризмом как через налагаемое на государства обязательство предотвращать террористические акты, которые потенциально могут оказать огромное негативное воздействие на права человека, так и посредством обязательства обеспечивать, чтобы любые контртеррористические мероприятия осуществлялись с соблюдением прав человека. В Глобальной контртеррористической стратегии Организации Объединенных Наций государства-члены вновь подтвердили эти обязательства, признав, в частности, что "действенные меры по борьбе с терроризмом и защита прав человека являются целями, которые не противоречат, а дополняют и взаимно подкрепляют друг друга".

54. К числу основных принятых под эгидой Организации Объединенных Наций универсальных документов по правам человека относятся Всеобщая декларация прав человека[41], Международный пакт о гражданских и политических правах и Международный пакт об экономических, социальных и культурных правах[42], а также ряд применимых протоколов.

55. Некоторыми региональными организациями также был выработан ряд конвенций, гарантирующих соблюдение прав человека. Примерами этого являются Европейская конвенция о защите прав человека и основных свобод (1950 год)[43], Американская конвенция о правах человека (1969 год)[44], Африканская хартия прав человека и народов (1981 год)[45] и Хартия основных прав Европейского союза (2000 год)[46].

56. Хотя всесторонний анализ вопросов, относящихся к сфере права в области прав человека, выходит за рамки настоящей публикации, соображения, касающиеся верховенства права, и применимые правовые документы будут рассмотрены в связи с конкретными мерами по борьбе с терроризмом, если это требуется с учетом контекста[47].

E. Региональные и субрегиональные правовые документы по вопросам борьбы с терроризмом

57. Помимо универсальных документов по борьбе с терроризмом, полезные материально-правовые и процессуальные стандарты криминализации актов терроризма, которые могут совершаться с использованием Интернета, содержатся в ряде региональных и субрегиональных документов. Эти документы, которые служат дополнением к универсальным документам

[41] Резолюция 217 A (III) Генеральной Ассамблеи.

[42] Резолюция 2200 A (XXI) Генеральной Ассамблеи, приложение.

[43] Council of Europe, *European Treaty Series*, No. 5.

[44] United Nations, *Treaty Series*, vol. 1144, No. 17955.

[45] Ibid., vol. 1520, No. 26363.

[46] *Official Journal of the European Communities*, C 364, 18 December 2000.

[47] См. также: Управление Организации Объединенных Наций по наркотикам и преступности, Часто задаваемые вопросы о международно-правовых аспектах борьбы с терроризмом, раздел V.

по борьбе с терроризмом, могут различаться по своему охвату и степени их обеспеченности правовой санкцией.

1. Совет Европы

58. В 2001 году Совет Европы выработал Конвенцию Совета Европы о киберпреступности[48], которая в настоящее время является единственным юридически обязывающим многосторонним документом по борьбе с преступной деятельностью, осуществляемой с использованием Интернета. Конвенция Совета Европы о киберпреступности направлена на приведение в соответствие национальных законов, касающихся киберпреступности, усовершенствование внутренних процедур выявления и расследования таких преступлений и уголовного преследования за их совершение, а также на создание оперативных и безотказных механизмов международного сотрудничества по этим вопросам[49]. В Конвенции устанавливаются общие минимальные стандарты в отношении внутренних преступлений, совершаемых с использованием компьютеров[50], и предусматривается уголовная ответственность за девять видов таких правонарушений, включая преступления, связанные с несанкционированным доступом к компьютерным системам, программам или данным и с противозаконным вмешательством в их работу; мошенничеством и подделкой документов с использованием компьютеров; а также с покушением на совершение таких актов, соучастием в их совершении или подстрекательством к ним[51].

59. Конвенция Совета Европы о киберпреступности также содержит важные положения процессуального характера, которые могут способствовать проведению расследований и сбору доказательств в связи с террористическими актами с использованием Интернета. Действие этих положений распространяется на любые уголовные преступления, совершаемые с помощью компьютера, а также на сбор доказательств в электронной форме, и они должны применяться с соблюдением надлежащих гарантий, предусмотренных нормами внутригосударственного права[52].

60. Например, Конвенция Совета Европы о киберпреступности обязывает ее участников принять законы, обязывающие провайдеров услуг Интернет, в случае поступления соответствующего требования со стороны сотрудников правоохранительных органов в ходе уголовного расследования или судебного разбирательства, сохранять хранящиеся на их серверах указанные данные в течение (возобновляемого) срока, не превышающего 90 дней[53], пока не будут приняты надлежащие правовые меры, принуждающие их к раскрытию таких данных[54]. Учитывая непостоянный характер электронных данных, а также то обстоятельство, что в случае транснациональных судебных дел традиционные процедуры оказания взаимной правовой помощи зачастую отнимают много времени, эта ускоренная процедура обеспечения сохранности соответствующих данных имеет ключевое значение[55]. Издание распоряжения

[48] Council of Europe, *European Treaty Series*, No. 185 (см. также по адресу: www.coe.int/cybercrime).

[49] Ibid., preamble.

[50] Пояснительная записка к Конвенции Совета Европы о киберпреступности, пункт 33. См. по адресу: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[51] Там же, статьи 2–8 и 11.

[52] Там же, подпункты *b)* и *c)* пункта 2 статьи 14 и статья 15. В число таких условий должна входить защита прав человека и свобод, в том числе прав, возникающих в связи с обязательствами, взятыми в рамках Европейской конвенции о защите прав человека и основных свобод, Международного пакта о гражданских и политических правах и других применимых международных документов по правам человека, а также надзор со стороны судебных или иных независимых органов.

[53] Любое обеспечение сохранности данных, предпринятое в ответ на просьбу о взаимной правовой помощи, производится на срок не менее 60 дней (Конвенция Совета Европы о киберпреступности, статья 29).

[54] Конвенция Совета Европы о киберпреступности, статья 16.

[55] Пояснительная записка к Конвенции Совета Европы о киберпреступности, пункт 157.

о сохранности данных или иные аналогичные меры также по ряду причин предпочтительны по сравнению с традиционными процедурами обыска и выемки, поскольку провайдеры услуг Интернет могут иметь больше возможностей для оперативного обеспечения сохранности улик, имеющих отношение к тому или иному делу. Кроме того, мера по обеспечению сохранности данных может в меньшей степени нарушать ход законной коммерческой деятельности провайдера услуг Интернет и в потенциале в меньшей степени воздействовать на репутацию его предприятия[56], что может способствовать налаживанию постоянного сотрудничества. Установленная согласно статье 19 Конвенции Совета Европы о киберпреступности процедура обыска и выемки в отношении хранимых данных предусматривает, применительно к хранимым данным, меры защиты, аналогичные тем, которые обычно обеспечиваются применительно к вещественным доказательствам[57] в рамках соответствующего внутригосударственного законодательства[58].

61. Конвенция Совета Европы о киберпреступности также требует, чтобы ее участники ввели в действие законодательство, касающееся представления хранимых данных об абонентах[59]. Такая информация может иметь решающее значение на стадии следствия, для того чтобы установить личность виновного в совершении террористического акта с использованием Интернета, и может включать сведения о физическом местонахождении такого лица, а также другие данные о сопутствующих коммуникационных услугах, использовавшихся при совершении данного террористического акта. Конвенция также требует от подписавших ее государств установить минимальные стандарты, позволяющие организовать в режиме реального времени сбор данных о потоках[60], связанных с конкретными сообщениями, а также перехват данных о контенте сообщений, касающихся определенных серьезных правонарушений, наказуемых согласно внутреннему законодательству[61].

62. В целях обеспечения правовой основы для сотрудничества в борьбе с использованием Интернета в террористических целях Конвенция Совета Европы о киберпреступности может применяться в сочетании с такими документами по борьбе с терроризмом, как Конвенция Совета Европы о предупреждении терроризма[62]. Конвенция Совета Европы о предупреждении терроризма обязывает участников криминализовать в соответствии с их национальным законодательством определенные деяния, такие как публичные провокации, вербовка и обучение, результатом которых может стать совершение террористических преступлений и каждое из которых может быть совершено с использованием Интернета. Конвенция также обязывает их принять меры к налаживанию сотрудничества на национальном и международном уровнях в целях предупреждения терроризма, в том числе при проведении следственных мероприятий. Например, в статье 22 Конвенции предусматривается обмен с другой стороной без предварительного запроса информацией, относящейся к расследованию или судебному разбирательству, в пределах, установленных внутренним законодательством, в общих интересах принятия ответных мер в связи с преступными действиями (добровольно передаваемая информация).

---

[56] Там же, пункт 155.

[57] Таким, как носители данных, на которых хранится информация.

[58] Пояснительная записка к Конвенции Совета Европы о киберпреступности, пункт 184.

[59] См. Конвенцию Совета Европы о киберпреступности, статью 18. Определение термина "сведения об абонентах" охватывает любую информацию, кроме данных о потоках или данных контента, касающуюся личности пользователя, его почтового или географического адреса, номера телефона и других средств доступа, сведений о выставленных ему счетах и произведенных им платежах, или любые другие сведения о месте установки коммуникационного оборудования, имеющиеся в соглашении об обслуживании с провайдером услуг Интернет.

[60] Согласно подпункту *d)* статьи 1 Конвенции Совета Европы о киберпреступности "данные о потоках" включают сведения, указывающие на происхождение, назначение, маршрут, время, дату, размер, продолжительность предоставления или вид базовой услуги.

[61] Согласно положениям соответственно статей 20 и 21 Конвенции Совета Европы о киберпреступности.

[62] Council of Europe, *Treaty Series*, No. 196. См. также по адресу: http://conventions.coe.int/Treaty/en/treaties/html/196.htm.

63. Конвенция Совета Европы о киберпреступности и Конвенция Совета Европы о предупреждении терроризма открыты для ратификации или присоединения к ним всех государств – членов Совета Европы[63], государств, не являющихся членами Совета Европы, которые участвовали в разработке этих конвенций, и других государств, не являющихся членами Совета Европы, которые получили предложение присоединиться к ним, с согласия всех государств, являющихся на данный момент участниками соответствующей Конвенции[64]. Стоит отметить, что ряд стран, официально не присоединившихся к Конвенции Совета Европы о киберпреступности, тем не менее использовали ее положения в качестве руководства при разработке собственного национального законодательства о борьбе с киберпреступностью (см. также раздел F, ниже, в отношении типового законодательства).

64. Совет Европы также выработал Дополнительный протокол к Конвенции о киберпреступности, касающийся криминализации актов расистского и ксенофобского характера, совершаемых с использованием компьютерных систем[65]. Этот Дополнительный протокол может также содействовать судебному преследованию за совершение с использованием Интернета террористических актов, имеющих целью подстрекательство к насилию по признаку расы, цвета кожи, происхождения, национальной или этнической принадлежности или вероисповедания[66]. Дополнительный протокол открыт для присоединения всех договаривающихся государств Конвенции Совета Европы о киберпреступности[67].

2. Европейский союз

65. В 2002 году Совет Европейского союза принял Рамочное решение 2002/475/ЈНА от 13 июня 2002 года о борьбе с терроризмом, унифицировавшее определение террористических преступлений во всех государствах – членах Европейского союза[68] путем введения конкретного и единого определения понятия "терроризм", установления юрисдикционных норм, гарантирующих возможность эффективного судебного преследования за совершение террористических преступлений, и формулирования специальных мер в отношении жертв террористических актов. В ответ на нарастание террористической угрозы, в том числе с использованием новых технологий, таких как Интернет, в 2008 году в рамочное решение 2002/475/ЈНА были внесены поправки[69], включавшие специальные положения, касавшиеся публичного подстрекательства к совершению террористических преступлений, вербовки в террористических целях и подготовки террористов. В этом решении Совет Европейского союза также учитывал резолюцию 1624 (2005) Совета Безопасности, в которой последний призвал государства принять меры, чтобы законодательно запретить подстрекательство к совершению террористического акта или актов и предотвращать такое поведение.

---

[63] По состоянию на дату выпуска настоящего издания членами Совета Европы являются следующие 47 государств: Австрия, Азербайджан, Албания, Андорра, Армения, Бельгия, Болгария, Босния и Герцеговина, бывшая югославская Республика Македония, Венгрия, Германия, Греция, Грузия, Дания, Ирландия, Исландия, Испания, Италия, Кипр, Латвия, Литва, Лихтенштейн, Люксембург, Мальта, Монако, Нидерланды, Норвегия, Польша, Португалия, Республика Молдова, Российская Федерация, Румыния, Сан-Марино, Сербия, Словакия, Словения, Соединенное Королевство, Турция, Украина, Финляндия, Франция, Хорватия, Черногория, Чешская Республика, Швейцария, Швеция и Эстония.

[64] См. Конвенцию Совета Европы о киберпреступности, статью 36, и Конвенцию Совета Европы о предупреждении терроризма, статьи 23–24.

[65] Council of Europe, *European Treaty Series,* No. 189.

[66] Ibid., art. 2.

[67] Ibid., art. 11.

[68] По состоянию на дату выпуска настоящей публикации членами Европейского союза являются следующие 27 государств: Австрия, Бельгия, Болгария, Венгрия, Германия, Греция, Дания, Ирландия, Испания, Италия, Кипр, Латвия, Литва, Люксембург, Мальта, Нидерланды, Польша, Португалия, Румыния, Словакия, Словения, Соединенное Королевство, Финляндия, Франция, Чешская Республика, Швеция и Эстония.

[69] Совет Европейского союза, Рамочное решение 2008/919/ЈНА от 28 ноября 2008 года, которым вносятся поправки в Рамочное решение 2002/475/ЈНА по борьбе с терроризмом.

66. Рамочное решение 2008/919/JHA создает основу для уголовного преследования также за распространение через Интернет террористической пропаганды и инструкций по изготовлению взрывных устройств постольку, поскольку распространение таких материалов осуществляется умышленно и отвечает критериям названных преступлений. Основанием для поправок к Рамочному решению 2002/475/JHA, касавшихся таких преступлений, как публичное подстрекательство, вербовка и подготовка террористов, послужили аналогичные положения Конвенции Совета Европы о предупреждении терроризма[70]. Рамочным решением 2008/919/JHA были введены новые составы преступлений, связанные с поведением, которое может вести к актам терроризма, независимо от способов или технических средств, с помощью которых совершаются такие преступления. Хотя положения Рамочного решения 2008/919/JHA, как и Конвенция Совета Европы о предупреждении терроризма, не ориентированы конкретно на деятельность в Интернете, они также охватывают деяния, совершаемые с использованием Интернета.

3. Дополнительные правовые документы

67. К числу принятых региональными или субрегиональными организациями дополнительных правовых документов обязательного характера, в которых могут содержаться положения о противодействии использованию Интернета террористами, относятся:

- Региональная конвенция Ассоциации регионального сотрудничества стран Южной Азии о пресечении терроризма (1987 год);
- Арабская конвенция о борьбе с терроризмом (1998 год);
- Договор о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с терроризмом (1999 год);
- Конвенция Организации Исламская конференция о борьбе с международным терроризмом (1999 год);
- Конвенция Организации африканского единства о предотвращении терроризма и борьбе с ним (1999 год);
- Межамериканская конвенция о борьбе с терроризмом (2002 год);
- Конвенция Ассоциации государств Юго-Восточной Азии по борьбе с терроризмом (2007 год);
- Директива по борьбе с киберпреступностью Экономического сообщества западноафриканских государств (2009 год).

F. Типовое законодательство

68. Хотя типовое законодательство, не создавая юридических обязательств, носит характер рекомендательных руководящих принципов, оно играет важную роль в процессе приведения в соответствие принятых государствами правовых стандартов. В отличие от международных конвенций, заключение которых может быть сопряжено с проведением обстоятельных переговоров в целях учета потребностей широкого круга потенциальных подписантов, положения типовых законов дают государствам возможность воспользоваться сводом

[70] Council of Ministers, "Amendment of the Framework Decision on combating terrorism", пресс-релиз от 18 апреля 2008 года.

эффективных базовых правовых норм в качестве отправной точки для разработки внутреннего законодательства. Главное преимущество использования типовых положений в качестве основы национального законодательства состоит в упрощении международного сотрудничества, в том числе за счет минимизации коллизий, возникающих в результате неверного истолкования норм в различных правовых системах (например, между юрисдикциями англосаксонского права и континентального права), а также в отношении критериев "двойной уголовной ответственности"[71]. (Обсуждение этого вопроса см. в разделе F.5 главы V, ниже.)

1. Содружество

69. Типовой закон Содружества о компьютерных преступлениях и связанных с компьютерами преступлениях (2002 год) был выработан на основе Конвенции Совета Европы о киберпреступности[72]. Цель этого Типового закона состоит в использовании сходных правовых традиций государств – членов Содружества[73] для содействия согласованию как материально-правовых, так и процессуальных аспектов борьбы с киберпреступностью и развитию международного сотрудничества. Типовой закон Содружества отвечает стандартам, установленным Конвенцией Совета Европы о киберпреступности.

2. Содружество Независимых Государств

70. Государства – члены Содружества Независимых Государств (СНГ) также приняли ряд типовых законодательных актов и руководящих принципов, направленных на согласование национальных законодательных систем с учетом международного опыта борьбы с терроризмом. В этих типовых положениях отражены международно-правовые стандарты, адаптированные к потребностям государств – членов СНГ[74]. Например, в статье 13 Типового закона об основах регулирования Интернета[75] содержатся типовые положения в отношении противодействия использованию Интернета в противоправных целях.

3. Международный союз электросвязи

71. Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций, играющим ведущую роль в вопросах киберпреступности. В целях содействия согласованию национального законодательства и процессуальных норм в отношении киберпреступности, включая террористические акты, совершаемые с использованием Интернета, МСЭ создал Инструментарий для разработки законодательства по киберпреступности (2010 год). Основой Инструментария стал комплексный анализ Конвенции

---

[71] Согласно принципу "двойной уголовной ответственности" выдача может быть допустима только в случаях, когда деяние, в связи с которым направляется запрос о выдаче, считается уголовно наказуемым как в запрашивающем, так и в запрашиваемом государстве.

[72] Дополнительные сведения см. по адресу: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

[73] По состоянию на дату выпуска настоящей публикации членами Содружества являлись следующие 53 государства: Австралия, Антигуа и Барбуда, Багамские Острова, Бангладеш, Барбадос, Белиз, Ботсвана, Бруней-Даруссалам, Вануату, Гайана, Гамбия, Гана, Гренада, Доминика, Замбия, Индия, Камерун, Канада, Кения, Кипр, Кирибати, Лесото, Маврикий, Малави, Малайзия, Мальдивские Острова, Мальта, Мозамбик, Намибия, Науру, Нигерия, Новая Зеландия, Объединенная Республика Танзания, Пакистан, Папуа-Новая Гвинея, Руанда, Самоа, Свазиленд, Сейшельские Острова, Сент-Винсент и Гренадины, Сент-Китс и Невис, Сент-Люсия, Сингапур, Соединенное Королевство, Соломоновы Острова, Сьерра-Леоне, Тонга, Тринидад и Тобаго, Тувалу, Уганда, Шри-Ланка, Южная Африка и Ямайка.

[74] По состоянию на дату выпуска настоящей публикации членами Содружества Независимых Государств являлись следующие 11 государств: Азербайджан, Армения, Беларусь, Казахстан, Кыргызстан, Республика Молдова, Российская Федерация, Таджикистан, Туркменистан, Узбекистан и Украина.

[75] Приложение к постановлению 36-9 Межпарламентской ассамблеи государств – участников Содружества Независимых Государств, принятому 16 мая 2011 года.

Совета Европы о киберпреступности и законов о киберпреступности, принятых в развитых странах[76]. Хотя Инструментарий МСЭ касается в первую очередь проблем кибербезопасности, он также содержит ряд типовых норм, позволяющих криминализовать отдельные акты терроризма, связанные с использованием Интернета, такие как несанкционированный доступ к компьютерным программам или данным в террористических целях либо распространение вредоносных программ в целях содействия терроризму[77].

[76] Международный союз электросвязи, Инструментарий для разработки законодательства по киберпреступности (2010 год), пункт 2.2.

[77] Там же, разделы 3 *f)* и 6 *h)*.

III. Политика и законодательные рамки

A. Введение

72. Помимо использования Интернета для планирования и финансирования террористических актов, террористы также используют его в целях вербовки и обучения новых членов; обмена сообщениями, проведения исследований или разведки потенциальных целей; распространения пропаганды; а также подстрекательства других к совершению террористических актов.

73. В настоящей главе рассматриваются вопросы, касающиеся выработки политики в области уголовного правосудия, а также направленного на противодействие этим угрозам законодательства в целях выявления на основе примеров и национального опыта, о которых сообщили ряд государств, представленных на совещаниях группы экспертов, общих проблем и подходов, которые могут либо препятствовать, либо способствовать эффективному расследованию дел в отношении актов терроризма, связанных с теми или иными аспектами использования Интернета, и уголовному преследованию за их совершение.

B. Политика

74. В целях обеспечения эффективности ответных мер органов уголовного правосудия в связи с угрозами, связанными с использованием Интернета террористами, государствам необходимы четкие национальные стратегии и соответствующая законодательная база. В общих чертах такие стратегии и законы должны быть направлены на:

a) криминализацию противоправных деяний, совершаемых террористами с использованием Интернета или связанных с ним служб;

b) предоставление следственных полномочий правоохранительным органам, расследующим дела, связанные с терроризмом;

c) регулирование связанных с Интернетом услуг (например, деятельности провайдеров услуг Интернет) и контроль контента;

d) содействие международному сотрудничеству;

e) выработку специальных процедур судопроизводства или доказывания;

f) поддержание международных стандартов в области прав человека.

Стратегические подходы

75. В своей публикации от 2011 года под названием "Борьба с использованием Интернета в террористических целях: правовые и технические вопросы"[78] Рабочая группа по противодействию использованию Интернета в террористических целях Целевой группы по

[78] См.: Организация Объединенных Наций, Целевая группа по осуществлению контртеррористических мероприятий, Рабочая группа по противодействию использованию Интернета в террористических целях, Борьба с использованием Интернета в террористических целях: правовые и технические вопросы (Нью-Йорк, 2011 год).

осуществлению контртеррористических мероприятий наметила три широких стратегических подхода, с помощью которых государства могут противодействовать деятельности террористов в Интернете, опираясь на:

a) законодательство общего характера по киберпреступности;

b) законодательство общего характера (не ориентированное специально на Интернет) о борьбе с терроризмом;

c) законодательство о борьбе с терроризмом, специально ориентированное на использование Интернета.

76. Следует отметить, что в рамках подхода *a)*, помимо применения законодательства общего характера по киберпреступности, при рассмотрении дел о террористической деятельности, связанной с теми или иными аспектами использования Интернета, в частности при расследовании предполагаемых действий, направленных на подстрекательство к совершению террористических актов, также могут применяться статьи, касающиеся других видов незавершенной преступной деятельности, таких как подстрекательство к совершению преступления и участие в преступном сообществе.

77. Используемая Рабочей группой широкая система классификации является практичной концептуальной основой для направления деятельности лиц, определяющих политику, а также законодателей при рассмотрении приемлемых для их конкретных государств политических и законодательных подходов.

78. Еще одним полезным ресурсом для лиц, определяющих политику, и законодателей, который упоминается в публикации "Борьба с использованием Интернета в террористических целях"[79], является выработанный под эгидой МСЭ Инструментарий для разработки законодательства по киберпреступности. В дополнение к другим типовым положениям в области уголовного права в Инструментарии предусмотрен ряд особых составов преступлений, связанных с терроризмом, в том числе в пункте *f)* раздела 3, который посвящен вопросам несанкционированного доступа к компьютерным программам или их приобретения в целях разработки, формулирования и планирования террористических актов, содействия и пособничества в их совершении, а также вступления в сговор о совершении или совершения актов терроризма.

79. В широких рамках, предусмотренных универсальными документами по борьбе с терроризмом и соответствующими международными нормами в области прав человека, правительствам предоставляется значительная степень гибкости в выборе предпочтительных подходов; поэтому подходы неизбежно различаются по государствам. В настоящей главе приводятся некоторые примеры подходов, принятых рядом государств, что может оказаться полезным для разработчиков политики и законодателей.

80. В настоящее время контртеррористическое законодательство, специально направленное против использования террористами Интернета как такового, выработано лишь в немногих государствах, однако существуют и такие, в том числе Соединенное Королевство, где после взрывов 2005 года в Лондоне правительство приняло Закон о терроризме 2006 года, в часть 1 которого включены положения, конкретно касающиеся деятельности на базе Интернета, которая, по-видимому, может подстрекать к совершению террористических актов или способствовать их совершению. Данный Закон дополняет Закон о неправомерном использовании компьютерных технологий 1990 года, в котором проблемы преступлений, совершаемых с использованием компьютеров, и киберпреступности рассматриваются в более общем плане.

[79] Там же, пункт 20.

81. В 2007 году в Объединенных Арабских Эмиратах были приняты федеральные законы, касающиеся Интернета и компьютерных правонарушений, которыми, помимо криминализации хакерства и других видов деятельности, связанных с Интернетом, устанавливалась уголовная ответственность за создание веб-сайтов или публикацию под вымышленными именами информации для террористических групп в целях содействия поддержанию контактов с их руководством или пропаганды их идеологии, финансирования их деятельности или же распространения информации о способах изготовления взрывчатых или иных веществ для использования при совершении террористических актов[80].

82. В 2008 году правительство Саудовской Аравии ввело в действие новые законы, касающиеся использования технологий, в том числе закон, которым в качестве уголовного преступления, наказуемого штрафами и лишением свободы на срок до 10 лет, признавалось владение веб-сайтами, пропагандирующими или поддерживающими терроризм[81].

83. Также в 2008 году правительство Пакистана приняло Указ о предупреждении электронных преступлений от 2008 года, которым вводились особые составы преступлений, связанных с кибертерроризмом. Данный Указ, однако, более не имеет силы[82].

84. Наконец, в том же году правительство Индии внесло поправки в Закон об информационных технологиях от 2000 года, чтобы ввести в него состав преступления "кибертерроризм" (статья 66F) и другие вопросы, связанные с использованием Интернета.

85. Тем не менее на международном уровне, в отсутствие каких-либо универсальных документов, налагающих прямое обязательство принять законодательство, специально направленное против деятельности террористов в Интернете, бóльшая часть правительств, за некоторыми исключениями, предпочитает бороться с такими угрозами, придерживаясь смешанного подхода, используя комбинацию общего уголовного законодательства и законодательства о борьбе с киберпреступностью и терроризмом. В ряде государств, например, главное внимание в уголовном законодательстве уделяется основным преступным деяниям без их дифференциации по конкретным средствам, с помощью которых они совершаются. В соответствии с этим подходом Интернет рассматривается лишь как средство, с помощью которого террористы совершают основные преступления, нередко обозначенные в положениях национального уголовного кодекса.

86. Этот подход характерен для Китая, где в Уголовном кодексе Китайской Народной Республики содержится статья о криминализации всех видов противоправной деятельности, связанных с использованием Интернета. Статьей 287 Уголовного кодекса устанавливается уголовная ответственность за использование компьютера при совершении преступления, судебное преследование и назначение наказания за которое будут осуществляться согласно соответствующим положениям данного Кодекса, касающимся криминализации и вынесения приговоров. Таким образом, в уголовном праве Китая использование Интернета рассматривается как одно из средств или орудий, с помощью которых может быть совершено преступное деяние, а не как самостоятельный составляющий элемент преступления, и, соответственно, уголовная ответственность за него устанавливается в рамках основных положений уголовного права.

87. Что касается терроризма, то в Китае действуют положения, криминализующие различные формы террористической деятельности, в том числе статья 120 Уголовного кодекса,

[80] Федеральный закон № (2) 2006 года о предупреждении преступлений с использованием информационных технологий, *Official Gazette of the United Arab Emirates*, vol. 442, 36th year, Muharam 1427 H/January 2006 (неофициальный перевод на английский язык см. по адресу: www.aecert.ae/pdfs/Prevention_of_Information_Technology_Crimes_English.pdf).

[81] David Westley, "Saudi tightens grip on Internet use", *Arabian Business*, 26 January 2008.

[82] "Pakistan lacks laws to combat cyber terrorism", *The New New Internet*, см. по адресу: www.thenewnewInternet.com/2010/09/01/pakistan-lacks-laws-to-combat-cyber-terrorism.

устанавливающая уголовную ответственность за деятельность, связанную с организацией террористических групп, руководством ими и участием в них. Это широкое положение о криминализации охватывает значительное число связанных с терроризмом видов деятельности, в том числе осуществляемых с использованием Интернета.

88. В Республике Корея в отношении террористических актов, в той или иной мере связанных с использованием Интернета, могут применяться два вида уголовного законодательства. Одним из них является общий уголовный кодекс, а другим – принятый в 1986 году специальный уголовный кодекс, касающийся преступных действий, связанных с использованием информационных/коммуникационных технологий. Статья 90 Уголовного кодекса касается подготовки таких актов, а также сговора, подстрекательства или пропаганды и предусматривает, что любое лицо, которое готовится к совершению или участвует в заговоре в целях совершения преступлений, предусмотренных статьей 87 Уголовного кодекса (массовые беспорядки, бунты или нарушения общественного порядка) или статьей 88 (убийства, совершаемые в целях подготовки деяний, предусмотренных статьей 87), подлежит тюремному заключению на срок три года или более. Согласно статье 101 Уголовного кодекса любое лицо, которое готовится или вступает в сговор в целях совершения преступления, предусмотренного статьями 92–99 Уголовного кодекса, считается виновным в совершении преступления и подлежит лишению свободы на два года или более. Статья 114 Уголовного кодекса касается организации преступной группы. Кроме того, в рамках специального уголовного кодекса правительство ввело ряд составов уголовных преступлений, установив уголовную ответственность непосредственно за совершение противоправных деяний, объектами которых являются информационно-коммуникационные сети и личная информация.

89. Как показывает опыт, когда речь идет о расследовании террористических актов и уголовном преследовании за их совершение, в том числе с использованием в той или иной степени Интернета, на практике большинство государств, независимо от провозглашаемой политической линии, придерживаются многостороннего подхода. Правоохранительные органы и органы прокуратуры используют любые законоположения, которые наилучшим образом соответствуют конкретным обстоятельствам дела.

90. Необходимые правоохранительным органам для эффективного расследования дел о терроризме полномочия во многом схожи, независимо от конкретной юрисдикции, о которой идет речь, а различия в национальной политике и законодательстве являются отражением многообразия правовых систем, конституционных положений и других факторов (например, культуры).

91. Область регулирования Интернета и управления информационными ресурсами оставляет значительный простор для разнообразия национальных подходов. В то время как международные стандарты, относящиеся к регулированию выражения и распространения тех или иных идей, содержатся во Всеобщей декларации прав человека и Международном пакте о гражданских и политических правах, никакого всеобъемлющего международно-правового документа обязывающего характера, которым бы устанавливались окончательные, обязательные нормы, указывающие, что́ следует считать надлежащим информационным наполнением Интернета или каким образом каждое государство должно регламентировать связанную с Интернетом деятельность в пределах собственной территории, не существует. В настоящее время детская порнография является единственной областью, деятельность в которой государства неизменно запрещают даже в отсутствие обязательного для всех документа или определения[83]. Что касается терроризма, однако, отсутствие универсально согласованного определения терроризма остается постоянным препятствием на пути к выработке какого-либо признанного на международном уровне подхода к надлежащей регламентации связанных с терроризмом деятельности и информационных ресурсов в Интернете.

[83] Maura Conway, "Terrorism and Internet governance: core issues", *Disarmament Forum*, vol. 3 (2007), p. 27.

92. Что касается специализированных процедур судопроизводства или доказывания в связанной с терроризмом области, то рядом государств приняты специальные процедуры судебного разбирательства и ведения дел о терроризме, которые могут также применяться в случаях, связанных с использованием террористами Интернета. При принятии такого подхода важно, чтобы любые специализированные механизмы в полной мере отвечали соответствующим международным обязательствам по защите прав человека, в том числе касающимся права на свободу и справедливое судебное разбирательство.

C. Законодательство

1. Криминализация

93. Как уже отмечалось выше, ни один из универсальных документов по борьбе с терроризмом не налагает на государства обязательство ввести в действие законодательство, специально направленное против использования Интернета террористами. Соответственно, в то время как весьма вероятно, что в большинстве случаев дела о терроризме будут в той или иной степени связаны с использованием правонарушителями Интернета, вполне вероятно и то, что во многих государствах, помимо применения положений о правонарушениях, связанных с противоправным поведением, конкретизированным в универсальных документах, органы власти также будут применять в целях привлечения к ответственности правонарушителей содержащиеся в их уголовных кодексах статьи о других уголовных преступлениях, в том числе о таких видах незавершенной преступной деятельности, как сговор, подстрекательство и участие в преступном сообществе.

94. В настоящем разделе рассматриваются примеры различных законодательных положений ряда государств в целях определения подходов, которые могли бы создать основу для принятия органами уголовного правосудия эффективных ответных мер в связи с различными видами деликтного поведения.

a) Совершаемые в Интернете деяния или размещаемые там заявления в поддержку терроризма

95. Помимо деяний, связанных с совершением террористических актов как таковых (например, бомбового терроризма), существуют явные свидетельства того, что Интернет все чаще используется террористами для осуществления таких вспомогательных мероприятий, как вербовка и обучение участников, обмен полезной информацией, распространение пропаганды и подстрекательство к совершению террористических актов. В силу конфигурации и глобального охвата Интернета становится все более вероятным, что в такие виды деятельности могут вовлекаться различные участники, физически находящиеся в разных судебных юрисдикциях.

96. В Соединенном Королевстве в части VI Закона о терроризме 2000 года предусмотрен ряд составов преступлений, которые могут стать основой для предъявления обвинений лицам, использующим Интернет в целях поддержки террористической деятельности.

97. Статьей 54 этого Закона устанавливается уголовная ответственность за проведение, прохождение или призыв других лиц к прохождению обучения или инструктажей по изготовлению или использованию огнестрельного оружия, радиоактивных материалов или оружия с их использованием, взрывчатых веществ или химического, биологического или ядерного оружия.

98. Статьей 57 устанавливается уголовная ответственность за владение соответствующими предметами в обстоятельствах, когда возникает обоснованное подозрение в том, что лицо владеет такими предметами в связи с подготовкой, подстрекательством к совершению или совершением террористического акта. За последние годы этот состав преступления был

успешно использован для судебного преследования ряда лиц, во владении которых были обнаружены такие разные предметы, как жесткие диски, DVD-диски и учебные материалы о способах изготовления или использования таких предметов, как минометы, жилеты смертника и напалм[84]. Для того чтобы факт совершения данного преступления был признан, обвинение должно доказать наличие связи между соответствующим предметом и конкретным террористическим актом. Известны несколько случаев успешного судебного преследования за преступления, предусмотренные статьей 57; однако, как видно из вынесенного решения в деле *Государство против Зафара, Батта, Икбала, Раджи и Малика* [2008 год], Апелляционный суд Англии и Уэльса, Отдел по уголовным делам, дело № 184, при толковании сферы применения данной статьи суды придерживаются более ограничительного подхода.

Государство против Зафара, Батта, Икбала, Раджи и Малика

Это дело, рассматривавшееся в 2007 году в Соединенном Королевстве, стало примером успешной апелляции подсудимых Зафара, Батта, Икбала, Раджи и Малика против осуждений, вмененных за обладание предметами в целях, связанных с совершением, подготовкой или подстрекательством к совершению террористического акта, в нарушение статьи 57 Закона о терроризме 2000 года.

Четверо из пяти обвиняемых по делу являлись студентами Брэдфордского университета. Пятый, Раджа, учащийся школы в Илфорде, установил контакт с Икбалом через службу обмена сообщениями MSN в Интернете.

Раджа на несколько дней приехал в Брэдфорд и остановился в доме, в котором проживали Икбал и Зафар. Раджа привез с собой три изготовленных им компакт-диска, содержавших выборки из материалов с компьютера и помеченных как "философские диски". По возвращении домой после этой поездки Раджа был арестован полицией.

По итогам проведенного полицией следствия были произведены аресты остальных обвиняемых и обыски по месту их жительства, в ходе которых выяснилось, что они также хранили радикальные джихадистские материалы, а также такие материалы, как загруженный из Интернета воинский устав армии Соединенных Штатов. Были обнаружены доказательства обмена посланиями через программу обмена сообщениями через Интернет, в том числе обсуждений между всеми четырьмя апеллянтами из Брэдфорда и живущим в Пакистане двоюродным братом Малика – Имраном.

Подсудимым первоначально были предъявлены обвинения по статье 58 Закона 2000 года; однако на этапе предания суду обвинение добавило в обвинительный акт ряд пунктов по статье 57 на основе тех же фактов, что и пункты обвинения по статье 58. После ряда досудебных постановлений суда по вопросу о том, может ли хранящаяся в электронном виде информация считаться предметом по смыслу статьи 57, обвинение предпочло продолжить судебное разбирательство только на основании обвинений по статье 57.

В ходе судебного разбирательства Зафар и Икбал были оправданы по одному пункту, в котором они обвинялись во владении тремя "философскими дисками", содержавшими полученные от Раджи материалы; однако вместе с другими обвиняемыми их признали виновными по всем остальным пунктам обвинения. Малик был приговорен к трем годам тюремного заключения, Зафар и Икбал – к трем годам заключения в учреждении для малолетних преступников, Батт – к 27 месяцам содержания под стражей и Раджа – к двум годам лишения свободы.

[84] Susan Hemming, "The practical application of counter-terrorism legislation in England and Wales: a prosecutor's perspective", *International Affairs*, vol. 86, No. 4 (July 2010), p. 963.

Эти приговоры были обжалованы подсудимыми. При рассмотрении апелляции суд пришел к заключению, что решающее значение имел вопрос о том, существовала ли, исходя из обстоятельств дела, связь между соответствующими предметами и террористическими актами, которая удовлетворяла бы критериям статьи 57.

Предметами, которые, по утверждению государственного обвинения, апеллянты хранили в нарушение статьи 57, были по большей части компакт-диски и жесткие диски, содержащие материалы в электронном виде. Данные материалы включали идеологическую пропаганду и переписку между подсудимыми, которые, по утверждению обвинения, свидетельствовали о наличии согласованного плана, предполагавшего поездку обвиняемых в Пакистан для прохождения обучения и участия в боевых действиях в Афганистане, что, по мнению государственного обвинения, было равноценно актам терроризма. Апелляционный суд постановил, что обвинению было необходимо сначала доказать, в каких целях каждый из апеллянтов владел хранимыми материалами, а затем доказать, что эти цели были "связаны с совершением, подготовкой или подстрекательством" к совершению предполагаемых обвинением террористических актов, а именно боевых действий против правительства Афганистана.

Исходя из обстоятельств дела, суд, отметив, что оно ставит ряд сложных вопросов толкования в отношении сферы применения статьи 57, постановил, что необходимой связи установлено не было, а следовательно, вынесенные в результате этого обвинительные приговоры были необоснованными, и удовлетворил апелляционные жалобы.

99. Статья 58 Закона оказалась особенно полезной в ряде случаев, когда органам власти было необходимо вмешаться из-за отсутствия каких-либо доказательств, что соответствующее лицо занимается связанной с терроризмом деятельностью. В данной статье устанавливается уголовная ответственность за сбор, изготовление или хранение, без уважительных причин, любых записей информации такого рода, которая, вероятно, была бы полезной для лица, совершающего или готовящегося к совершению террористического акта, или за хранение любых документов или записей, содержащих такую информацию.

100. В деле *Государство против К.* [2008 год], 3 All ER 526, суд постановил, что документ подпадает под действие статьи 58, только если есть вероятность, что по своему характеру он может принести практическую пользу лицу, совершающему или готовящемуся совершить террористический акт. Этот подход был подтвержден в решении по делу *Государство против Г. и Дж.* [2009 год], Палата лордов Соединенного Королевства, № 13, когда суд подтвердил данный "критерий практической пользы", согласно которому хранение документов или записей является преступлением, только если последние могут быть использованы на практике, а соответствующее лицо хранит их без уважительной причины[85]. Никаких ограничений в отношении того, что в этих целях можно считать разумным оправданием, не существует, при условии что это может быть по закону признано обстоятельством, освобождающим от ответственности.

101. В соответствии со статьей 58 от стороны обвинения не требуется доказывать, что обвиняемый является террористом или что он владеет какими-либо предметами в террористических целях; однако обращаться для доказывания практической полезности того или иного предмета к доказательствам, лежащим вне документа, обвинение может лишь в очень

[85] Ibid., p. 962.

ограниченном числе случаев. Например, в качестве доказательства может быть истребован шифр для расшифровки закодированного документа, однако истребование каких-либо доказательств для объяснения того, зачем обведены кружками какие-либо места на карте, не допускается. Информация должна "говорить сама за себя", а не носить характера общераспространенных сведений.

102. В деле *Государство против Султана Мохаммеда* [2010 год], Апелляционный суд Англии и Уэльса, Отдел по уголовным делам, дело № 227, суд постановил, что "[п]ри условии, что документ, содержащий соответствующую информацию, не относится к числу находящихся в повседневном пользовании обычных членов общества (например, опубликованные расписания и карты), и при условии, что разумно мыслящие присяжные могли бы обоснованно прийти к заключению, что в этом документе содержится такая информация, которая, вероятно, будет полезной для лица, совершающего или готовящегося совершить террористический акт, задачей присяжных будет определить, убеждены ли они в том, что данный документ содержит такую информацию. Если это так, и при условии наличия у подсудимого необходимого преступного умысла (mens rea), останется выяснить только вопрос о том, имеется ли у подсудимого какая-либо уважительная причина"[86]. Соответственно, коллегия присяжных должна решить, действительно ли данное подсудимым объяснение причины хранения соответствующего документа является разумным оправданием с учетом конкретных фактов и обстоятельств дела[87].

103. Законом о терроризме 2006 года был введен (в его статье 5) состав преступления "совершение действий по подготовке к проведению террористического акта". Данная статья предназначена для рассмотрения дел, связанных с ситуациями, когда лица, активно планировавшие совершение террористических актов, были остановлены, прежде чем они совершили или попытались совершить террористический акт как таковой[88].

104. Статья 5 оказалась особенно полезной при рассмотрении дел "волков-одиночек", когда преступник действует в одиночку, когда нет достаточных доказательств для обоснования обвинения в сговоре ввиду невозможности доказать причастность более чем одного лица или когда органам власти неизвестны детали планировавшегося преступления. В связи с этим составом преступления не требуется доказательства совершения могущего быть идентифицированным завершенного террористического акта или актов, однако обвинение обязано доказать наличие конкретного намерения совершить террористический акт или помочь другим сделать это. В Соединенном Королевстве за совершение этого преступления несколько человек были осуждены и приговорены к различным срокам лишения свободы вплоть до пожизненного тюремного заключения[89].

105. Одним из примеров полезности таких положений, как статья 58, является дело *Государство против Теренса Роя Брауна* [2011 год], Апелляционный суд Англии и Уэльса, Отдел по уголовным делам, дело № 2751.

[86] Выдержка из решения по делу "R. v. Muhammed [2010] EWCA Crim 227: terrorism – preparing an act of terrorism", *Criminal Law and Justice Weekly* (20 March 2010).

[87] Hemming, "The practical application of counter-terrorism legislation in England and Wales", p. 963.

[88] Ibid., p. 964.

[89] Ibid.

Государство против Теренса Роя Брауна

Теренс Рой Браун, гражданин Соединенного Королевства, являлся владельцем интернет-магазина, в котором он рекламировал и продавал ежегодное издание компакт-диска, который он назвал "Поваренная книга анархиста" (идентично хорошо известной книге под тем же названием). Однако в отличие от какого-либо единого издания, на этих дисках содержались 10 322 файла, и некоторые из них представляли собой полноценные самостоятельные публикации. К их числу относились учебные пособия для террористов, такие как «Наставление для членов "Аль-Каиды"» и инструкции по изготовлению различных видов взрывчатых веществ и взрывных устройств. Среди других файлов были руководства по изготовлению ядов, способам избежать привлечения к себе внимания органов власти во время поездок, а также методам обращения с оружием. Явно пытаясь обойти закон, г-н Браун разместил на рекламировавшем данную публикацию веб-сайте заявления об отказе от ответственности, указывая, что выполнение содержащихся в ней инструкций может быть незаконным или опасным и что они предназначены для "приятного чтения и имеют лишь историческую ценность". В ходе следствия стало ясно, что в своей деятельности г-н Браун исходил из чисто коммерческих интересов. Было также установлено, что он сознательно расширил свою коллекцию сразу после взрывов в Лондоне в июле 2005 года и тем самым значительно увеличил свою прибыль.

В марте 2011 года г-н Браун был признан виновным по семи пунктам обвинения согласно Закону о терроризме 2000 года (статья 58), относящимся к сбору информации, которая могла бы быть использована для подготовки или совершения террористических актов, по двум пунктам обвинения согласно Закону о терроризме 2006 года (статья 2), касающимся распространения террористических публикаций, а также в совершении преступления, предусмотренного Законом о доходах от преступной деятельности 2002 года, связанного с передачей имущества, нажитого преступным путем (использование им прибыли от своей коммерческой деятельности)[a].

Выдвинутое г-ном Брауном в ходе судебного разбирательства оправдание сводилось к тому, что его деятельность представляла собой не более чем законное осуществление своего права на свободу выражения в отношении материала, имеющегося в свободном доступе в Интернете и сходного если не по объему, то по своему типу с тем, который продается в других книжных интернет-магазинах. Те же доводы приводились при безуспешной попытке обжаловать вынесенный приговор, когда суд постановил, что ограничение предусмотренных в статье 10 прав г-на Брауна в отношении материала, который, вероятно, мог способствовать террористам, было оправданным и пропорциональным. Суд также подтвердил дискреционное право органов уголовного преследования не предъявлять обвинение каждому, кто, возможно, совершил преступление, но вместо этого рассматривать каждое дело по существу.

---

[a] "Businessman who published bomb-makers' handbook 'facing lengthy spell in jail'", *Daily Mail*, 9 March 2011. См. по адресу: www.dailymail.co.uk/news/article-1364621/Businessman-published-bomb-makers-handbook-facing-lengthy-spell-jail.html#ixzz1j4gXbMLu.

106. Это дело является одним из нескольких, включая *дело Государство против К.* [2008 год], Суд королевской скамьи, дело № 827, и дело *Государство против Г.* [2010 год], 1-й Апелляционный суд, дело № 43, в рамках которых суды в Соединенном Королевстве проясняют судебную практику в отношении сферы действия и применимости статьи 58 данного Закона в свете надлежащих гарантий в области прав человека.

107. Помимо уголовных составов преступления, предусмотренных антитеррористическим законодательством, органы власти Соединенного Королевства, когда того требуют обстоятельства, успешно применяют в целях судебного преследования лиц, занимающихся связанной с терроризмом деятельностью, такой состав преступления, как подстрекательство. Примером такого подхода является дело *Государство против Билала Захира Ахмада*[90], в рамках которого подсудимый был осужден за подстрекательство к убийству.

Государство против Билала Захира Ахмада

Это дело в суде Соединенного Королевства связано и последовало за слушавшимся в 2010 году делом Рошанары Чоудри, которую 2 ноября 2010 года приговорили к пожизненному заключению за покушение на убийство члена парламента Стивена Тиммса.

В одном из выступлений Чоудри заявила, что приняла решение совершить преступление примерно за четыре недели до нападения в мае 2010 года и, готовясь к нему, купила два ножа, один как запасной на случай, если первый сломается, когда она ударит жертву. Она рассказала полиции, что в период своей радикализации просматривала видеозаписи Анвара аль-Авлаки и Абдуллы Аззама и посещала веб-сайт www.revolutionmuslim.com. На этом широко известном сайте, который был размещен в Соединенных Штатах, содержались материалы, пропагандировавшие насильственный джихад, в том числе видеозаписи и речи с призывами к терроризму, а также ссылки на веб-сайты с террористическими публикациями.

1 ноября 2010 года подсудимый разместил на своей странице в Facebook ссылку на новостное сообщение о деле Тиммса/Чоудри, к которой он добавил следующий комментарий:

Эта сестра посрамила нас, мужчин. ЭТО ДОЛЖНЫ ДЕЛАТЬ МЫ.

4 ноября 2010 года подсудимый разместил на веб-сайте Revolution Muslim статью под названием "Члены парламента, голосовавшие за войну в Ираке за подписью "БИЛАЛ". В заголовке статьи содержался символ Исламского государства Ирак (филиала "Аль-Каиды"). А ее текст начинался с цитаты из Корана, гласящей, что те, кто умирает, не приняв участие в джихаде, это лицемеры.

В статье читателям сообщалось, что они могут "отследить" членов британского парламента с помощью приведенной в ней ссылки на официальный сайт парламента. Это дало бы им возможность выяснить подробности в отношении подходящего места, где членов парламента можно "встретить лично" для проведения над ними "хирургических операций".

За этим следовали 29 цитат из религиозных текстов, все в переводе на английский язык и все в связи с обязанностью мусульман участвовать в джихаде или "принять мученичество". Непосредственно после цитат была приведена ссылка на веб-страницу с рекламой продажи ножей. Один экземпляр этой статьи был зафиксирован в электронной форме в качестве вещественного доказательства британскими сотрудниками по борьбе с терроризмом. Еще одна копия веб-страницы была получена в ответ на запрос из компании Google Inc.

[90] Nottingham Crown Court, 13 May 2011.

10 ноября 2010 года подсудимый был арестован сотрудниками подразделения по борьбе с терроризмом полиции Уэст-Мидлендс неподалеку от своего дома в Вулвергемптоне. При нем был обнаружен ноутбук, который, как он сообщил производившим арест сотрудникам, он использовал для размещения статьи о членах парламента на сайте Revolution Muslim. Судебная экспертиза ноутбука показала, что перед арестом подсудимый, по-видимому, пытался удалить следы своей деятельности в Интернете.

16 ноября подсудимому были предъявлены обвинения в подстрекательстве к убийству в связи с его статьей, а также по трем пунктам преступного хранения материалов, которые могут быть использованы террористами, согласно статье 58 Закона о терроризме 2000 года. Позже он признал себя виновным по этим пунктам обвинения, а также в преступном возбуждении религиозной ненависти, что проявилось в его комментариях в интернет-форуме, и был приговорен к 12 годам тюремного заключения и дополнительно к пяти годам нахождения на пробации.

108. В Соединенных Штатах в соответствии с параграфом 842 *p)* раздела 18 Кодекса Соединенных Штатов, озаглавленным "Распространение информации, касающейся взрывчатых веществ, разрушительных устройств и оружия массового уничтожения", считается противозаконным, если какое-либо лицо тем или иным способом распространяет информацию, касающуюся изготовления или использования взрывчатых веществ, разрушительных устройств или оружия массового уничтожения, с намерением использовать данную информацию в целях содействия совершению насильственного преступления или зная, что лицо, которому передается данная информация, предполагает использовать ее в целях содействия совершению насильственного преступления. Это законоположение применяется в Соединенных Штатах в целях уголовного преследования лиц, распространяющих такую информацию с использованием Интернета.

b) Подстрекательство

109. Такое преступление, как подстрекательство к совершению террористических актов, является предметом резолюции 1624 (2005) Совета Безопасности. В этой резолюции Совет призвал все государства, в частности, принять такие меры, которые могут быть необходимы и уместны и будут соответствовать их обязательствам по международному праву, чтобы законодательно запретить подстрекательство к совершению террористического акта или актов и предотвращать такое поведение.

110. Разработка и применение законов, криминализующих подстрекательство к совершению террористических актов, но при полном обеспечении защиты прав человека, таких как права на свободу выражения и ассоциации, остаются постоянной проблемой для разработчиков политики, законодателей, правоохранительных органов и прокуратуры. Дела, которые связаны с заявлениями лиц в Интернете, особенно когда предполагаемые правонарушители, используемые ими интернет-службы и их целевая аудитория находятся в разных юрисдикциях, регулируются различными национальными законами и конституционными гарантиями и, соответственно, создают дополнительные проблемы для следователей и обвинителей в плане осуществления международного сотрудничества.

111. Международный опыт в области правоприменения в отношении уголовных преступлений, связанных с подстрекательством к совершению террористических актов, высвечивает два вопроса: во-первых, насколько важно (а иногда и трудно) на практике провести различие между террористической пропагандой (заявлениями, пропагандирующими определенные идеологические, религиозные или политические воззрения) и материалами или заявлениями, представляющими собой подстрекательство к совершению террористических актов; и

во-вторых, насколько применение законов, касающихся предполагаемых актов подстрекательства, требует тщательной, по каждому отдельному пункту, оценки обстоятельств и контекста в целях определения, является ли возбуждение судебного преследования по статье за подстрекательство уместным в том или ином конкретном случае.

112. На совещании группы экспертов те из них, которые имели опыт участия в делах, связанных с расследованием и судебным преследованием по статьям о подстрекательстве к совершению террористических актов, были согласны с этим и подчеркивали, как важно на практике в полном объеме оценить контекст, в котором делались предполагаемые заявления подстрекательского характера, включая не только их формулировки, но и аудиторию, на которую они были ориентированы, а также указывали, что особенности вероятных адресатов информации могут быть крайне важными факторами для определения того, стоит ли в том или ином конкретном случае возбуждать уголовное дело по обвинению в подстрекательстве и какова вероятность того, что оно будет успешным.

113. В Соединенном Королевстве в соответствии со статьей 59 Закона о терроризме 2000 года преступлением считается подстрекательство другого лица к совершению террористического акта полностью или частично за пределами Соединенного Королевства, когда такое деяние, будь оно совершено в Англии и Уэльсе, являлось бы одним из преступлений, предусмотренных в данной статье (например, убийство, умышленное нанесение ран, взрывы или создание угрозы жизни в результате повреждения имущества).

114. В широко известном деле *Государство против Тсули и других*[91] Юнис Тсули, Васим Мугал и Тарик аль-Даур признали себя виновными по обвинению, согласно Закону о терроризме 2000 года, в подстрекательстве к убийству в террористических целях путем создания и содержания большого количества веб-сайтов и чат-форумов, которые использовались для публикации материалов, направленных на подстрекательство к совершению убийств в террористических целях, в первую очередь в Ираке.

Государство против Тсули и других

Участниками этого широко известного дела, слушавшегося в Соединенном Королевстве, были трое подсудимых – Юнис Тсули, Васим Мугал и Тарик аль-Даур, которым первоначально были предъявлены обвинения по 15 пунктам. До начала суда Тсули и Мугал признали себя виновными по обвинению в сговоре в целях совершения обманных действий. В ходе судебного разбирательства, выслушав свидетельские показания со стороны обвинения, все трое признали себя виновными по обвинению в подстрекательстве к терроризму за рубежом, а аль-Даур признал себя виновным по обвинению в сговоре с целью обмана.

В период с июня 2005 года и до их ареста в октябре 2005 года подсудимые занимались покупкой, конструированием и содержанием большого числа веб-сайтов и чат-форумов в Интернете, на которых публиковались материалы, направленные на подстрекательство к совершению убийств в террористических целях, в первую очередь в Ираке. Расходы на приобретение и обслуживание веб-сайтов покрывались из доходов от мошенничества с кредитными картами. В числе размещаемых на веб-сайтах материалов были заявления, что долгом мусульман является ведение вооруженного джихада против евреев, крестоносцев, богоотступников и их приспешников во всех мусульманских странах и что обязанность каждого мусульманина – сражаться и убивать их, будь то гражданские лица или военные, где бы они не находились.

[91] *R v. Tsouli* [2007] EWCA (Crim) 3300.

В чат-форумах в Интернете лицам, склонным присоединиться к мятежникам, предоставлялась информация о маршрутах проезда в Ирак и инструкции по пользованию оружием и изготовлению взрывчатых веществ. По месту жительства у каждого из подсудимых были изъяты экстремистские идеологические материалы, свидетельствующие о приверженности усвоенным ими оправдывающим убийства взглядам, насаждаемым на веб-сайтах и в чат-форумах.

Аль-Даур организовал добычу краденых кредитных карт как для своих собственных нужд, так и для обеспечения Мугала средствами в целях создания и содержания веб-сайтов. Аль-Даур был также причастен к другим мошенническим действиям с кредитными картами, доходы от которых не использовались на содержание веб-сайтов. Убытки компаний – эмитентов кредитных карт от этого аспекта мошеннической деятельности подсудимых составили 1,8 млн. фунтов стерлингов.

Среди вещественных доказательств был собственноручно составленный Тсули и обнаруженный в его письменном столе список, в который он заносил сведения о ряде веб-сайтов и об украденных кредитных картах. С помощью этого списка были выявлены 32 отдельных веб-сайта, предоставленных различными компаниями, специализирующимися на веб-хостинге, которые Тсули создал или пытался создать в основном в последнюю неделю июня, но также в июле и августе 2005 года. Создание и администрирование этих веб-сайтов финансировались за счет незаконного использования сведений о кредитных картах, которые были похищены у владельцев счетов путем либо прямого хищения компьютерных записей, либо посредством взлома защиты компьютеров, либо тех или иных мошеннических операций внутри финансовых учреждений. Эти сведения о кредитных картах Тсули передавали два других обвиняемых.

Созданные Тсули веб-сайты использовались в качестве средства для загрузки джихадистских материалов, подстрекавших к совершению актов насилия вне пределов Соединенного Королевства – в Ираке. Доступ к этим сайтам был ограничен кругом лиц, которым были предоставлены имя пользователя и пароль. По заключению судьи первой инстанции, это было сделано для того, чтобы веб-хостинговым компаниям и правоохранительным органам было труднее узнать, что именно размещается на данных сайтах.

5 июля 2007 года Тсули был приговорен к десяти годам и трем с половиной годам лишения свободы (по совокупности) по двум пунктам обвинения. Мугал – к семи с половиной и трем с половиной годам лишения свободы (по совокупности) по двум пунктам обвинения, а аль-Даур – к шести с половиной и трем с половиной годам лишения свободы (по совокупности).

115. В части 1 Закона о терроризме 2006 года введен ряд новых составов преступлений в целях расширения возможностей принятия органами власти соответствующих мер в случаях, когда те или иные лица выступают с заявлениями, подстрекающими к совершению террористических актов или прославляющими их или иным образом направленными на содействие совершению таких актов.

116. В соответствии с частью 1 данного Закона устанавливается уголовная ответственность для лиц, публикующих сообщения, прямо или косвенно направленные на поощрение рядовых членов общества к подготовке террористических актов, подстрекательству к совершению или совершению таких актов, в том числе (но не только) на поощрение в форме "прославления" террористических актов, либо для лиц, опрометчивое поведение которых может иметь такой эффект. На практике то, как, вероятно, следует понимать соответствующее заявление, определяется в зависимости от его содержания в целом и от контекста, в котором оно было сделано.

117. В статье 2 Закона устанавливается уголовная ответственность за распространение (умышленное или необдуманное) террористических изданий. Последние определяются как публикации, которые могут побуждать к совершению актов терроризма или могут быть полезны лицам, планирующим или совершающим такие акты. Эта вторая категория охватывает те же типы документов или публикаций, к которым применима статья 58 Закона о терроризме 2000 года. Как и в статье 1 Закона о терроризме 2006 года, вопрос о том, подпадает ли рассматриваемый материал под определение "террористических публикаций", должен решаться с учетом его содержания в целом и условий, в которых он становится доступным[92].

118. В Соединенном Королевстве при принятии решений о целесообразности возбуждения уголовного преследования за подстрекательство обвинители пользуются широкими дискреционными полномочиями, учитывая при этом право на свободу слова, а также общий контекст, в котором готовятся или распространяются соответствующие заявления или публикации, в том числе и то, как они могут быть поняты как широкой общественностью, так и целевой аудиторией.

119. В Соединенных Штатах используется иной правовой подход в отношении криминализации актов подстрекательства к терроризму и судебного преследования за их совершение в силу предусмотренных Первой поправкой к Конституции конституционных гарантий, которые касаются осуществления права на свободу слова. В соответствии с принципами, изложенными в решении по делу *Бранденбург против штата Огайо*, 395 US. 444 (1969), в целях обеспечения успеха уголовного преследования индивидуума за подстрекательство к совершению преступных деяний (включая терроризм) обвинение обязано доказать как наличие намерения подстрекать кого-то или добиться совершения противоправного деяния, так и вероятность того, что определенные высказывания на самом деле способны побудить кого-либо к неминуемому совершению противоправных действий[93].

120. В рамках судебного преследовании за высказывания, подстрекающие к совершению террористических актов, компетентные органы в Соединенных Штатах опираются на статьи о таких видах неоконченной преступной деятельности, как подстрекательство и участие в сговоре, наряду с положениями Уголовного кодекса Соединенных Штатов о "материальной поддержке", которые в определенных обстоятельствах позволяют возбуждать уголовное преследование за поведение, предполагающее поддержку насильственных актов терроризма[94].

121. Положениями параграфов 2339A и 2339B раздела 18 Уголовного кодекса Соединенных Штатов об оказании материальной поддержки соответствующим лицам запрещается сознательно или преднамеренно предоставлять, покушаться на предоставление или вступать в сговор в целях предоставления материальной поддержки или ресурсов террористическим организациям. Законом об объединении и укреплении Америки путем создания соответствующих механизмов, необходимых для предупреждения и пресечения терроризма (закон PATRIOT) 2001 года было расширено определение понятия материальной поддержки, которое теперь охватывает "любое имущество, материальное или нематериальное, или услуги, включая... обучение, экспертные консультации или помощь... или коммуникационное оборудование"[95].

[92] Hemming, "The practical application of counter-terrorism Законодательство in England and Wales", p. 963.

[93] Elizabeth M. Renieris, "Combating incitement to terrorism on the Internet: comparative approaches in the United States and the United Kingdom and the need for an international solution", *Vanderbilt Journal of Entertainment and Technology Law,* vol. 11, No. 3 (2009), pp. 681-682.

[94] United States Criminal Code, title 18, sections 2339A and 2339B.

[95] Renieris, "Combating incitement to terrorism on the Internet", pp. 682-683.

122. Включенные в параграф 373 *a)* раздела 18 Уголовного кодекса Соединенных Штатов составы уголовных преступлений, такие как подстрекательство или участие в сговоре, предусматривают, что в подстрекательстве может быть обвинено любое лицо, которое "подстрекает, отдает приказы, склоняет или иначе пытается убедить другое лицо принять участие в поведении, квалифицируемом как фелония, с намерением добиться, чтобы это другое лицо совершило такое деяние".

123. В Соединенных Штатах слушалось несколько дел, в рамках которых такой подход был успешно применен в целях судебного преследования за слова или действия террористов в Интернете. К их числу относится дело *Соединенные Штаты Америки против Эмерсона Уинфилда Биголли*.

Соединенные Штаты Америки против Эмерсона Уинфилда Биголли

Двадцатидвухлетний студент (гражданин Соединенных Штатов) Эмерсон Уинфилд Биголли был обвинен в причастности к распространению через Интернет информации, касающейся изготовления взрывных устройств, и подстрекательству к совершению насилия на американской территории. Среди дополнительных обвинений против него также были нападение на агентов Федерального бюро расследований (ФБР) и угрозы им заряженным огнестрельным оружием.

Официально известный под псевдонимом Асадулла аль-Шишани, Биголли принимал активное участие в имеющем международную известность англоязычном джихадистском форуме под названием "Ансар аль-Муджахидин" и в конечном счете стал там одним из активных модераторов. Форум предоставлял Биголли возможности для выражения своей приверженности радикальным взглядам и одновременно для поощрения других единоверцев к участию в террористических актах на территории Соединенных Штатов. Его пропагандистская деятельность также включала распространение видеоматериалов с инструкциями по изготовлению взрывных устройств в целях совершения террористических актов. В число намечаемых целей входили синагоги, военные объекты, железнодорожные линии, полицейские участки, мосты, мачты сотовой связи и водоочистные сооружения.

За девять месяцев Биголли опубликовал ряд длинных сообщений, в которых подробно рассматривался вопрос о необходимости насилия. В обвинительном акте, вынесенном 14 июля 2011 года Окружным судом Соединенных Штатов по Восточному округу штата Вирджиния, в качестве основного доказательства фигурировала часть пропагандистского материала, размещенного Биголли в интернет-форуме:

> Мирные протесты не работают. Куфары[a] видят единственное решение своих проблем в войне, поэтому и мы должны считать войну решением наших проблем. Никакого мира. Только пули, бомбы и акты мучеников.

Он также разместил в Интернете ссылки на доступный для скачивания документ под названием "Учебный курс по взрывчатым веществам". Этот 101-страничный документ, автором которого являлся "шейх-мученик профессор Абу Хаббаб аль-Мисри" (как его называет Биголли), содержит подробные инструкции по созданию лаборатории с основными химическими ингредиентами для производства взрывчатых веществ. К нему было добавлено примечание, предупреждавшее, что для собственной защиты лицам, загружающим эту информацию, следует позаботиться об использовании программного обеспечения, обеспечивающего анонимность.

Все это время Биголли находился под постоянным наблюдением федеральных властей. Один из агентов ФБР скачал документ по одной из приведенных ссылок, что в конечном счете привело к аресту Биголли. 14 апреля 2011 года ему было предъявлено обвинение в противозаконном и целенаправленном распространении через Интернет информации, связанной с изготовлением и распространением взрывчатых материалов, применением оружия массового уничтожения и подстрекательством к совершению взрывов в общественных местах, правительственных зданиях и системах общественного транспорта. 9 августа 2011 года Биголли признал себя виновным в подстрекательстве к совершению террористических актов. В настоящее время он ожидает вынесения приговора.

[a] Один из терминов, широко использовавшихся Биголли в ходе дискуссий на интернет-форумах применительно к "неверующим" или "неверным".

c) Обзор подхода к подстрекательству с правовой точки зрения

124. В Европе статья 3 Рамочного решения 2008/919/ПВА Совета Европейского союза от 28 ноября 2008 года о внесении поправок в Рамочное решение 2002/475/ПВА о борьбе с терроризмом и статья 5 Конвенции Совета Европы о предупреждении терроризма обязывают соответствующие государства-члены каждого из документов ввести уголовную ответственность за действия или заявления, представляющие собой подстрекательство к совершению террористических актов. Конвенция Совета Европы о предупреждении терроризма налагает на государства-члены обязательство криминализовать "публичное подстрекательство к совершению преступлений террористического характера", а также как вербовку, так и подготовку террористов.

125. В процессе осуществления Конвенции, которая частично основана на положениях статьи 3 Дополнительного протокола к Конвенции Совета Европы о киберпреступности, касающегося криминализации актов расизма и ксенофобии, совершаемых с применением компьютерных систем, государства обязаны добиваться разумного баланса между потребностями правоохранительных органов и защитой прав человека и свобод. Соответственно, это порождает существенные проблемы и споры. Тем не менее статья 5 (как и статьи 6 и 7, касающиеся вербовки и обучения в террористических целях) должна применяться в сочетании с основным положением статьи 12, предусматривающим, что эту криминализацию надлежит осуществлять таким образом, чтобы было обеспечено соблюдение прав человека, в частности прав на свободу выражения, свободу ассоциации и свободу вероисповедания, закрепленных в документах по правам человека, в том числе в пункте 1 статьи 10 Европейской конвенции о защите прав человека и основных свобод.

126. Европейский суд по правам человека, оценивая средства защиты, предоставляемые в пункте 1 статьи 10 Европейской конвенции о защите прав человека и основных свобод, уже рассматривал положения статьи 5 Конвенции Совета Европы о предупреждении терроризма. В решении по широко известному делу *Леруа против Франции*[96] французский суд не увидел нарушения статьи 10 в случае, когда журналист был признан виновным и оштрафован за публикацию некоей карикатуры в баскском еженедельнике. 11 сентября 2001 года карикатурист представил в редакцию журнала рисунок, изображавший нападение на башни-близнецы Всемирного торгового центра, с подписью, пародировавшей рекламный слоган известного бренда: "Мы все мечтали об этом... ХАМАС это сделал" (ср. "Sony это сделала"). Затем этот рисунок был опубликован в журнале 13 сентября 2001 года.

[96] Judgement by the European Court of Human Rights (Fifth Section), case of *Leroy v. France*, Application no. 36109/03 of 2 October 2008.

127. В своих обоснованиях вынесенного решения Европейский суд по правам человека, в частности, ссылался на статью 5 Конвенции Совета Европы о предупреждении терроризма, и это был первый случай, когда Суд принял во внимание положения этой Конвенции в своем решении. Он постановил, что автор рисунка пошел дальше простой критики Соединенных Штатов и, скорее, поддерживал и восхвалял их насильственное разрушение. Суд отметил, что сопровождавшая рисунок подпись указывает на моральную поддержку подозреваемых в совершении терактов 11 сентября 2001 года со стороны заявителя. К числу других факторов, принятых во внимание Судом, относились выбранная заявителем формулировка подписи, дата публикации рисунка (что, по мнению Суда, усугубляло ответственность карикатуриста) и то обстоятельство, что рисунок был распространен в политически нестабильном регионе (Стране Басков). Согласно заключению Суда данная карикатура вызвала определенный общественный резонанс, способный побудить к насилию и свидетельствующий о вероятности воздействия на общественный порядок в регионе. Принципы, выработанные в решении по этому знаковому делу, будут в равной степени применимы к случаям, когда предполагаемое подстрекательство к терроризму осуществляется с использованием Интернета.

128. В Европе известен ряд случаев успешного судебного преследования за связанные с подстрекательством деяния. Например, в Германии в 2008 году курд Ибрагим Рашид, иммигрант из Ирака, был признан виновным в подстрекательстве по обвинению в ведении "виртуального джихада" в Интернете. По утверждению обвинения, размещая пропагандистские материалы "Аль-Каиды" в интернет-чатах, Рашид пытался вербовать людей для вступления в ряды "Аль-Каиды" и участия в джихаде.

129. В изданном ЮНОДК Обзоре дел о терроризме[97] содержится полезная сводка подходов к криминализации актов подстрекательства, принятых в Алжире, Египте, Испании и Японии. В Алжире, в соответствии с пунктом 1 статьи 87-бис Уголовного кодекса, совершение террористических актов карается смертной казнью, пожизненным заключением либо лишением свободы на другие длительные сроки. В пункте 4 статьи 87-бис предусматривается, что лица, оправдывающие перечисленные террористические акты, подстрекающие к их совершению или финансирующие их, подлежат наказанию в виде лишения свободы на сроки от 5 до 10 лет, а также штрафа[98].

130. В Египте, согласно статье 86bis Уголовного кодекса, преступлениями считаются деяния, равнозначные ответственности за осуществление и поддержку, планирование и подготовка террористических актов, членство в нелегальных организациях или поддержка таковых, предоставление финансирования и материальной поддержки террористическим организациям, а также подстрекательство к совершению преступлений. Кроме того, данной статьей предусматривается ужесточение наказаний, в частности, за преднамеренное содействие (любыми средствами) достижению целей террористических организаций или за приобретение или производство (прямо или косвенно) предметов, публикаций или записей любого рода, предназначенных для содействия достижению таких целей или их поощрения[99].

131. В Японии любое лицо, подстрекающее, прямо или через посредника, к совершению преступления, подлежит такому же наказанию, как если бы данное лицо являлось одним из фактических исполнителей преступления (статья 61 Уголовного кодекса)[100]. Другими законоположениями в Японии, такими как статьи 38–40 Закона о предотвращении подрывной деятельности, устанавливается уголовная ответственность за подстрекательство к мятежу или поджогу в целях пропаганды и поддержки какой-либо политической доктрины или политики или противодействия им.

[97] Управление Организации Объединенных Наций по наркотикам и преступности, Обзор дел о терроризме (2010 год).

[98] Там же, пункт 100.

[99] Там же, пункт 111.

[100] Там же, пункт 100.

132. В Испании, в соответствии со статьями 18 и 579 испанского Уголовного кодекса, публичное подстрекательство к совершению преступления, связанного с терроризмом, рассматривается как подготовительный этап преступной провокации. Статьей 578 предусматривается наказание за преступление "восхваление терроризма"; этот состав преступления был введен в Уголовный кодекс Органическим законом № 7/2000 от 22 декабря 2000 года. В неофициальном переводе эта статья гласит, что "восхваление или оправдание, с использованием любых средств публичного выражения мнений и распространения информации, преступлений, предусмотренных в статьях 571–577 настоящего Кодекса (Террористические преступления), или любых лиц, принимавших участие в их исполнении или совершении действий, связанных с дискредитацией, оскорблением или унижением жертв террористических преступлений или членов их семей, подлежат наказанию в виде лишения свободы на срок от одного до двух лет". Органическим законом также предусматривается наказание в виде поражения в гражданских правах на определенный срок по приговору суда[101].

133. В Индонезии не существует норм, специально касающихся деятельности, которую террористы ведут с использованием Интернета, включая подстрекательство к совершению террористических актов. В статье 14 Закона № 15/2003 о пресечении актов терроризма подстрекательство к совершению террористических актов рассматривается без упоминания об использовании преступниками конкретных способов связи, как и в Уголовном кодексе Индонезии, в котором рассматриваются вопросы подстрекательства к совершению других преступных деяний. Компетентные органы Индонезии успешно осуществляют судебное преследование лиц за связанную с терроризмом деятельность в Интернете. В 2007 году 24-летний Агунг Прабово, также известный как Макс Фидерман, был приговорен к трем годам лишения свободы (согласно подпункту *c)* пункта 13 постановления правительства, принятого взамен Закона № 1/2002 и Закона № 15/2003 о пресечении актов терроризма) за регистрацию и хостинг веб-сайта www.anshar.net по просьбе лидера террористической группы "Джемаа Исламия" Нурдина М. Топа, переданной ему через посредника Абдула Азиза. По имеющимся сведениям, Азиз по просьбе Топа создал сайт www.anshar.net в середине 2005 года в целях распространения джихадистской пропаганды. Наряду с тем что на нем выложена общая информация об исламе и джихаде, он также содержит специальные "советы и рекомендации" о том, как и где проводить теракты, с предложениями в отношении маршрутов, ведущих к торговым центрам и административным зданиям, сведениями о дорожных пробках и конкретными наименованиями мест скопления граждан[102]. По другому делу к пяти годам лишения свободы за соучастие в совершении террористического акта был приговорен Мухаммад Джибрил Абдул Рахман, известный также как Мухаммад Рикки Ардан (Принц джихада).

134. В Сингапуре в контексте использования Интернета подпункт *g)* пункта 2 статьи 4 сингапурского Свода правил пользования услугами Интернета запрещает распространение материалов, "восхваляющих этническую, расовую или религиозную ненависть, рознь и нетерпимость, подстрекающих к ним или одобряющим их".

2. Соображения с точки зрения верховенства права в отношении криминализации подстрекательства

135. Призывая государства криминализировать подстрекательство к совершению террористических актов, резолюция 1624 (2005) Совета Безопасности прямо предусматривает, чтобы государства обеспечили соответствие любых мер, принимаемых ими для выполнения своих обязательств, всем их обязательствам по международному праву, в частности по праву в области прав человека, беженскому праву и гуманитарному праву.

[101] Там же, пункт 115.

[102] См. www.indonesiamatters.com/624/wwwansharnet-chatroom-jihad.

136. Данный принцип, также нашедший свое отражение в универсальных документах по борьбе с терроризмом и многократно подтвержденный на международном уровне (в том числе в рамках Организации Объединенных Наций), является одним из основополагающих элементов принятого ЮНОДК подхода с позиций "верховенства права" в целях усиления ответных мер, предпринимаемых в связи с терроризмом органами уголовного правосудия в рамках универсального правового режима борьбы с терроризмом, и находит поддержку в многочисленных региональных документах по борьбе с терроризмом и правам человека, особенно в упоминавшихся выше документах, выработанных Советом Европы (см. раздел D главы II, выше)[103].

137. В рамках настоящей публикации невозможно в полном объеме проанализировать, с точки зрения соблюдения гарантированных прав человека на свободу выражения мнений, все доступные комментарии и судебные прецеденты, касающиеся надлежащего предметного охвата и сферы применения уголовных статей, которые приняты странами в целях криминализации подстрекательства к совершению террористических актов.

138. Однако в то время как доступная юриспруденция в отношении точной сферы применения таких положений международных документов по правам человека, как пункт 1 статьи 10 Европейской конвенции о защите прав человека и основных свобод и статья 19 Международного пакта о гражданских и политических правах, оставляет место для непрекращающихся споров, ясно то, что на практике установление надлежащего баланса между сохранением права на свободу выражения мнений и применением уголовного законодательства, направленного против подстрекательства к совершению террористических актов, по-прежнему остается проблемой для правительств.

3. Правомочия правоохранительных органов

139. В ходе расследования дел о терроризме, связанных с использованием подозреваемыми в терроризме Интернета или других соответствующих услуг, нередко возникает потребность в принудительных действиях в виде проведения обыска, установления наблюдения и контроля со стороны служб разведки и правоохранительных органов. Поэтому для успеха любого судебного преследования очень важно, чтобы применение этих методов ведения следствия было надлежащим образом санкционировано в рамках национальных законов и чтобы, как и всегда, базовым законодательством была предусмотрена поддержка основных прав человека, защищенных согласно нормам международного права в области прав человека.

a) Полномочия производить обыски, вести наблюдение и прослушивание линий связи

140. В Израиле вопрос о полномочиях для ведения расследования в целях сбора цифровых улик в Интернете как по общеуголовным делам, так и по делам, связанным с терроризмом, решается на основе Закона о компьютерах 1995 года, которым определен ряд конкретных полномочий по сбору цифровых улик. Законом о компьютерах была внесена поправка в Закон

[103]См. доклады Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Совету по правам человека и Генеральной Ассамблее, в которых Специальный докладчик выражал обеспокоенность по поводу возможного воздействия, которое направленное против подстрекательства законодательство может оказать на свободу слова и выражения, способствуя криминализации свободы высказываний, не являющихся подстрекательством к терроризму. Эти взгляды и обеспокоенность были подчеркнуты в письменном сообщении Управления Верховного комиссара Организации Объединенных Наций по правам человека, представленном на совещании группы экспертов; см. также Совместную декларацию о свободе выражения мнений и Интернете, опубликованную 1 июня 2011 года Специальным докладчиком по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, Представителем Организации по безопасности и сотрудничеству в Европе по вопросам свободы средств массовой информации, Специальным докладчиком Организации американских государств по вопросу о свободе выражения мнений и Специальным докладчиком Африканской комиссии по правам человека и народов по вопросу о свободе выражения мнений и доступе к информации в Африке, в которой они вновь подтвердили основополагающее значение права на свободу выражения мнений.

о перехвате телефонных разговоров, согласно которой завладение информацией, обмен которой производился между соответствующими компьютерами, считается одной из форм "перехвата", что, таким образом, позволяет следственным органам получить разрешение судебных или, в безотлагательных и исключительных случаях, административных органов на получение данных, передаваемых в процессе обмена информацией между компьютерами.

141. В 2007 году был принят Закон о передаче данных. Цель этого законодательного акта состояла в том, чтобы упорядочить, сделав ее более структурированной и прогрессивной, принятую практику в отношении получения данных, не касающихся содержания передаваемой информации, от компаний, обеспечивающих проводную и сотовую телефонную связь, а также от организаций, обеспечивающих доступ в Интернет. Действие данного Закона не распространяется на интернет-провайдеров, предоставляющих услуги другого рода, такие как хранение информации, обмен информацией, электронная почта, социальные сети и тому подобное. В настоящее время в случаях, когда компетентные органы желают получить информацию от провайдеров услуг Интернет, применяется старая статья закона, в целом позволяющая соответствующим органам издавать повестки о вызове в суд и получать информацию от тех, кто располагает сведениями, которые могут помочь следствию.

142. В 2010 году правительство Израиля представило законопроект, направленный на кодификацию положений, определяющих следственные полномочия в отношении как вещественных, так и цифровых данных. Данный законопроект был разработан в целях организации сбора цифровых улик на современной основе. Законопроект предусматривает упорядоченное распределение полномочий, которые в настоящее время в израильском законодательстве не прописаны. Это, например, проведение тайных обысков компьютеров (в случае особо тяжких преступлений), извлечение информации, подлежащей хранению (в будущем) на определенном компьютере, порядок получения хранящихся в электронной почте сообщений, находящихся в распоряжении провайдера услуг Интернет, а также, при определенных обстоятельствах, обыск содержащихся в компьютерах материалов с разрешения административных органов. Если законопроект будет принят, то эти меры будут применяться при расследовании дел о терроризме, связанных с использованием Интернета.

143. В 2006 году правительство Франции приняло новое законодательство о борьбе с терроризмом, упрощающее процесс ведения наблюдения за средствами связи в целях расследования дел, связанных с терроризмом, а также доступ полиции к получению передаваемых данных у операторов телефонной связи, провайдеров услуг Интернет и администрации интернет-кафе.

144. Законом о борьбе с терроризмом и о ряде положений по вопросам безопасности и пограничного контроля (№ 2006-64 от 23 января 2006 года) предусмотрено, что в случаях, связанных с расследованием предполагаемой террористической деятельности, провайдеры услуг Интернет, интернет-кафе, провайдеры и операторы услуг по размещению информации должны сообщать специализированным правительственным учреждениям данные о трафике, вызывавшихся номерах и IP-адресах.

145. В соответствии со статьей 6 операторы мобильной связи и интернет-кафе обязаны сохранять данные учета клиентских подключений в течение 12 месяцев и предоставлять их в распоряжение полиции. Кроме того, законом разрешается использование камер видеонаблюдения в общественных местах, таких как вокзалы, церкви и мечети, магазины, заводы и атомные электростанции. Статья 8 позволяет полиции вести автоматический контроль за транспортными средствами и пассажирами на дорогах и шоссе Франции (в том числе делать фото номерных знаков автомобилей и их пассажиров), а также вести наблюдение за гражданами на крупных общественных мероприятиях[104].

[104] www.edri.org/edrigram/number4.2/frenchlaw

146. Несколько позже, 14 марта 2011 года, были внесены поправки во французский Уголовно-процессуальный кодекс, которыми органам власти были предоставлены дополнительные полномочия по расследованию дел о терроризме. Эти поправки включают право на реквизицию относящихся к расследованию документов (в том числе на преобразование и перенос компьютерных данных), расшифровку защищенных компьютерных данных, проникновение в цифровую среду, захват компьютерных данных (включая изображения), прослушивание телефонных переговоров и перехват других сообщений. Кроме того, этот закон создает правовую основу для деятельности сотрудников правоохранительных органов, в частности участвующих в групповых дискуссиях в Интернете в рамках расследования преступлений, связанных с подстрекательством к терроризму. Это один из важных правовых вопросов, который правительства, возможно, пожелают рассмотреть. Эти статьи, кроме того, предоставляют французским правоохранительным органам возможность добывать улики, связанные с данными о подключениях электронной почты, телефонных переговорах и IP-адресах.

147. Эксперт из Китая упомянул о действующих в этой стране правилах, согласно которым полиция при проведении уголовных расследований, связанных с использованием Интернета, вправе предписать провайдерам услуг Интернет и операторам связи через Интернет предоставить относящиеся к делу документы и данные, которые они, по закону, обязаны сохранять в течение 60 дней.

148. В Соединенном Королевстве Законом о регулировании следственных полномочий 2000 года созданы правовые рамки, регламентирующие осуществляемые государственными учреждениями пять видов деятельности по ведению наблюдения:

- перехват сообщений (например, прослушивание телефонных разговоров или получение доступа к содержанию электронной почты);
- интрузивные методы наблюдения (например, негласное наблюдение в частных помещениях или транспортных средствах);
- целенаправленное наблюдение (например, негласное наблюдение за указанным объектом в общественном месте);
- использование тайных осведомителей (например, секретных агентов) как источников информации;
- сбор коммуникационных данных (например, учетных данных, касающихся передачи сообщений, но не содержания таких сообщений)[105].

149. Помимо изложения целей таких видов деятельности и описания процедур, необходимых для их санкционирования, данный Закон обязывает органы наблюдения учитывать, насколько соразмерными являются осуществление этих полномочий и посягательство на права лиц, находящихся под наблюдением, и принять меры к избежанию того, что называется "побочным следствием вмешательства" и в результате чего нарушаются права сторон, не являющихся объектами наблюдения. Законом также устанавливается уголовная ответственность сторон, в распоряжении которых находятся ключи шифрования целевых коммуникаций, за отказ передать такие ключи уполномоченным органам[106].

150. В 2000 году правительство Индии приняло Закон об информационных технологиях 2000 года, в который в 2008 году оно внесло поправки, предусматривавшие введение состава преступления "кибертерроризм" (статья 66F) и охватывавшие ряд других вопросов, касающихся Интернета. Пункт 1 статьи 67C Закона посвящен вопросу о сохранении данных и

[105] "Summary of surveillance powers under the Regulation of Investigatory Powers Act", National Council for Civil Liberties.

[106] Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007), p. 216.

предусматривает, что подлежащие регулированию провайдеры услуг Интернет "должны защищать и хранить такую информацию, которая может быть указана, в течение такого срока и в таком виде и формате, которые могут быть предписаны центральным правительством", а также объявляет преступлением (наказуемым лишением свободы на срок до трех лет и штрафом) сознательное нарушение данного обязательства.

151. В пункте 1 статьи 69 Закона правительственные структуры наделяются полномочиями издавать распоряжения о "перехвате, мониторинге и дешифровке любой информации, формируемой, передаваемой, получаемой или хранимой на любых компьютерных ресурсах" и устанавливаются правовые обязательства и гарантии, относящиеся к таким действиям государства, а в пункте 1 статьи 69A государственным учреждениям предоставляется право издавать распоряжения о блокировании открытого доступа к любой информации через компьютерные ресурсы, если, по их мнению, это необходимо или целесообразно сделать в интересах суверенитета, целостности, безопасности Индии и ее международных отношений или в целях предупреждения подстрекательства к совершению соответствующих "подсудных" правонарушений, включая акты терроризма. Наконец, в статье 69B специально назначенные государственные учреждения наделяются полномочиями контролировать, собирать и хранить трафик данных или информацию, создаваемую, передаваемую либо получаемую с помощью любых компьютерных ресурсов.

152. В Новой Зеландии Закон об обысках и наблюдении 2012 года обновляет, укрепляет и унифицирует полномочия правоохранительных органов, касающиеся производства обысков, установления наблюдения и перехвата сообщений с учетом появления новых видов технологий. В этом Законе сформулировано новое определение термина "обыски компьютерных систем", в соответствии с которым сфера его охвата распространяется на обыски компьютеров, внутренне не связанных с сетью, но способных получать к ней удаленный доступ.

153. В целях укрепления правовых гарантий в Законе поясняется, что обыск компьютеров с использованием удаленного доступа допускается только в двух случаях: когда компьютер имел возможность на законных основаниях получать доступ к компьютерной системе, являющейся предметом обыска, и, следовательно, рассматривается как часть этой системы; и когда отсутствует фактическое месторасположение, подлежащее обыску (например, в случае электронной почты на базе интернет-технологий, к которой пользователь получает доступ из различных мест, таких как интернет-кафе). Законом также предусматривается, что, когда сотрудники полиции проводят санкционированные обыски объектов, содержащих данные из Интернета, с использованием удаленного доступа, они обязаны направить уведомление в электронной форме о проведении обыска по адресу электронной почты обыскиваемого объекта.

b) Проблемы, связанные с предоставлением возможности прослушивать линии связи

154. При проведении мероприятий по электронному мониторингу, наблюдению или перехвату компетентным органам потребуется содействие операторов, обеспечивающих услуги связи общего пользования или связанные с этим услуги. В то время как во многих случаях частные операторы готовы предоставлять помощь выполняющим свои законные функции сотрудникам правоохранительных органов, очевидно, что существуют ограничения по времени и объему ресурсов, которые частные операторы могут расходовать на безвозмездной основе. Поэтому желательно, чтобы правительствами были созданы четкие правовые основы обязательств, налагаемых на стороны, принадлежащие к частному сектору, включая технические требования, предъявляемые к их сетям, а также порядок погашения затрат, связанных с предоставлением таких возможностей.

155. В Израиле статья 13 Закона о коммуникациях 1982 года гласит, что премьер-министр вправе предписать провайдерам услуг Интернет на территории Израиля осуществить

технологические изменения, требуемые силами безопасности (включая полицию, органы безопасности и другие специальные службы) в целях борьбы с терроризмом. Действие этого Закона распространяется только на провайдеров услуг Интернет, которые, согласно израильским законам, получают лицензии Министерства связи. Он не применяется в отношении действующих в Израиле провайдеров услуг по хранению данных или по управлению контентом, поскольку этим компаниям лицензии Министерства не требуются.

156. В Новой Зеландии в Законе 2004 года о средствах телекоммуникации (возможности для перехвата сообщений) уточняются обязательства операторов сетей по содействию уполномоченным государственным органам в проведении операций перехвата или по предоставлению этим органам разрешенной информации, относящейся к телефонным звонкам. Закон обязывает операторов сетей обеспечить, чтобы каждая телекоммуникационная сеть или служба общественного пользования, находящаяся в их собственности, под их контролем или управлением, располагала возможностями для перехвата информации. Считается, что сети или службы обладают такими возможностями, если уполномоченные государственные органы способны с их помощью перехватывать дистанционные сообщения или сервисы таким путем, который позволяет идентифицировать и перехватить только намеченное сообщение, получить данные о вызове и его содержании (в пригодной к использованию форме), а также осуществить перехват незаметно, своевременно и эффективно, не нарушая неприкосновенности частной жизни других пользователей телекоммуникационных услуг и не допуская чрезмерного вмешательства в их деятельность. Закон также обязывает операторов сетей предоставлять средства для дешифровки любых сообщений, дистанционно передаваемых через их сети, если содержание сообщения зашифровано, а средство шифрования было предоставлено оператором соответствующей сети.

157. Учитывая, что некоторым сетевым операторам для выполнения этих требований потребуется время и они понесут определенные расходы, в Законе предусматривается предоставление операторам, которых это затрагивает, от 18 месяцев до пяти лет (в зависимости от состояния сети) для создания вышеупомянутых возможностей. Кроме того, правительство согласилось покрыть расходы по созданию возможностей для перехвата в сетях, которые на дату начала операции уже находились в эксплуатации, но у которых необходимые возможности перехвата отсутствовали.

158. В Бразилии официальный перехват телефонных сообщений, осуществляемый уполномоченными государственными учреждениями, регулируется Федеральным законом № 9.296 1996 года, а также статьей 5 (XII) Федеральной конституции 1988 года. Признавая неприкосновенный характер телекоммуникаций, эти законы предусматривают, при наличии разрешения суда, специальные исключения в целях проведения уголовных расследований или уголовных процессов. Закон устанавливает процедуры, которым необходимо следовать в случае перехвата телефонных разговоров, который осуществляется под контролем судьи. По завершении прослушивания его результаты надлежит транскрибировать и представить судье вместе с краткой сводкой всех действий, предпринятых в рамках предоставленных полномочий (статья 6).

159. В целях выполнения своих юридических обязательств телекоммуникационные компании должны создать и подготовить специализированные подразделения и инвестировать средства в необходимые технологии. Что касается затрат на обеспечение возможностей перехвата, то на телекоммуникационные компании ложится обязанность по обеспечению необходимых технических ресурсов и персонала для поддержки санкционированных мероприятий по перехвату. Данный подход отражает тот факт, что, согласно конституции Бразилии, телекоммуникационные компании функционируют на основе концессионных договоров с правительством и предоставление телекоммуникационных услуг считается общественной услугой.

160. В Индонезии после взрывов на Бали в 2002 году правительство приняло законодательство о борьбе с терроризмом, которое позволяет правоохранительным органам и органам

безопасности в целях проведения связанных с терроризмом расследований перехватывать и изучать информацию, которая выражается, пересылается, получается или хранится в электронном виде или с использованием оптических устройств. Что касается сроков хранения интернет-файлов или журналов регистрации, то этот вопрос регулируется Законом № 11 от 2008 года об электронной информации и электронных транзакциях, а конкретно подпунктом a пункта 1 его статьи 6, который обязывает, чтобы в каждой системе, управляемой провайдером услуг электронных систем, в полном объеме воспроизводились и хранились в течение предусмотренного законом срока любая электронная информация и/или электронные документы.

161. В Алжире в 2006 году правительство приняло закон, разрешающий ведение наблюдения с помощью скрытых микрофонов и видеокамер и перехват переписки, если это санкционировано прокурором и осуществляется под его непосредственным контролем. Тем же законом разрешается использование методов внедрения агентов в целях расследования дел, связанных с терроризмом или организованной преступностью, а агентам в процессе внедрения позволяется совершать определенные незначительные правонарушения. Тайна личности агента тщательно охраняется законом, но его внедрение должно осуществляться под контролем ведущего расследование прокурора или судьи[107].

162. В Малайзии Закон о коммуникациях и мультимедийных средствах 1998 года содержит ряд положений, относящихся к регулированию Интернета и связанных с ним уголовных расследований. Например, в статье 249 данного Закона, касающейся вопроса о доступе к компьютерной информации в ходе обысков, предусматривается, что в понятие доступа входит получение "паролей, кодов шифрования или дешифрования, программного или аппаратного обеспечения и любых других средств, необходимых для обеспечения возможности понимания хранящихся в памяти компьютера данных".

163. Кроме того, положениями главы 4 данного Закона, которая касается вопросов, затрагивающих национальные интересы, на операторов интернет-услуг налагается общее обязательство приложить "максимум усилий" в целях обеспечения того, чтобы предоставляемые ими сетевые ресурсы не использовались для совершения любых преступлений, подпадающих под действие законодательства Малайзии (статья 263), и предусматривается, что соответствующий министр вправе принимать решения, с указанием необходимых технических требований, обязывающих обладателя лицензии или отдельную категорию обладателей лицензий использовать свои возможности для обеспечения санкционированного перехвата сообщений (статья 265).

164. Глава 2 Закона касается вопроса о вредоносных информационных ресурсах и запрещает провайдерам услуг по предоставлению контента, а также любым лицам, которые пользуются такими услугами, предоставлять контент "непристойного, порнографического, лживого, угрожающего или оскорбительного характера, с тем чтобы вызвать раздражение, оскорбить, угрожать или причинить беспокойство какому-либо лицу" (статья 211). Лица, нарушающие эти обязательства, совершают правонарушение и подлежат наказанию в виде штрафа в размере не более 50 тыс. ринггитов (около 16 200 долл. США) или тюремного заключения на срок не более одного года, либо в виде того и другого, а также подлежат наложению текущего штрафа в размере 1000 ринггитов (около 325 долл. США) за каждый день или часть дня, в течение которых продолжается совершение правонарушения после вынесения приговора. В статье 212 Закона предусматривается назначение органа из представителей отрасли, который будет являться форумом для выработки отраслевого кодекса, касающегося содержания информационных ресурсов.

[107] Управление Организации Объединенных Наций по наркотикам и преступности, Обзор дел о терроризме, пункт 215.

165. В Соединенных Штатах операторы средств телекоммуникации в настоящее время обязаны, по Закону 1994 года о содействии правоохранительным органам со стороны системы коммуникаций, обеспечивать возможности для прослушивания телефонных линий и перехвата информации в широкополосных сетях.

c) Регламентирование работы интернет-кафе

166. Согласно имеющимся свидетельствам террористы в некоторых случаях пользуются услугами интернет-кафе для совершения действий, связанных с терроризмом; однако нет никаких данных относительно той доли, которую данная деятельность составляет по отношению к законной деятельности в Интернете, осуществляемой с использованием этих услуг.

167. Вопрос о том, в какой степени правительствам следует в целях борьбы с терроризмом регулировать Интернет или интернет-кафе, весьма сложен и тесно связан с проблемами прав человека. В подходах к нему на международном уровне имеются расхождения. В ряде государств, в том числе в Египте, Индии, Иордании и Пакистане, правительства применяют специальные меры законодательного или регулятивного характера, обязывающие операторов интернет-кафе получать, хранить и предоставлять сотрудникам правоохранительных органов, по их запросам, фотографии, удостоверяющие личность клиентов, а также их адреса и данные об использовании ресурсов/подключениях.

168. Хотя правительства вправе налагать на операторов интернет-кафе обязательства, направленные на ограничение злоупотреблений их услугами со стороны террористов, о полезности таких мер можно спорить, особенно с учетом существования других общедоступных интернет-услуг (таких, как компьютеры в публичных библиотеках или общественные зоны (Wi-Fi) беспроводного доступа в Интернет), которые могут обеспечить аналогичные возможности для анонимного использования Интернета террористами. Следует отметить, что правительство Италии в 2005 году наложило на операторов интернет-кафе нормативные обязательства, касавшиеся идентификации клиентов; однако в конце 2010 года эти правила были отменены, отчасти из-за опасений по поводу воздействия, которое эта форма регулирования может оказать на развитие интернет-услуг и их потребление законными пользователями.

d) Контроль контента

169. Вопрос о том, в какой степени правительствам следует регулировать связанный с терроризмом контент в Интернете, является крайне спорным. Подходы здесь существенно различаются, причем некоторые государства применяют механизмы жесткой регламентации деятельности провайдеров услуг Интернет и других сопутствующих услуг, в том числе в ряде случаев используют технологические средства для фильтрации определенного контента или блокирования доступа к нему. Другие придерживаются менее жесткого подхода к регулированию, в большей степени опираясь на саморегулирование в информационном секторе.

170. В статье "Терроризм и Интернет: нужно ли закрывать веб-сайты, пропагандирующие терроризм?"[108] Барбара Мэнтел отмечает, что "большинство провайдеров услуг Интернет, веб-хостинговых компаний, файлообменных сайтов и сайтов социальных сетей имеют соглашения об условиях предоставления услуг, которые запрещают размещение определенного контента". Например, отмечает она, служба размещения информации "Сети для малого бизнеса" компании Yahoo специально запрещает абонентам использовать данную службу в целях предоставления материальной поддержки или ресурсов любой организации или организациям, которые правительство Соединенных Штатов признало иностранными террористическими организациями. В этом смысле в рамках информационного общества существует элемент саморегулирования.

[108] Barbara Mantel, "Terrorism and the Internet: should web sites that promote terrorism be shut down?", *CQ Global Researcher*, vol. 3, No. 11 (November 2009).

171. Оценивая подходы и уровни вмешательства в этой области, правительствам следует учитывать ряд факторов, в том числе местонахождение ресурса, на котором размещена информация, конституционные или иные гарантии, касающиеся права на свободу выражения мнения, само содержание контента, а также стратегические последствия, с точки зрения разведывательных или правоохранительных органов, организации мониторинга или фильтрования определенных сайтов или прекращения доступа к ним[109].

172. В Соединенном Королевстве одно из инновационных инструментальных средств, доступных полномочным органам при решении дел о предполагаемых актах подстрекательства с использованием Интернета, предусмотрено в статье 3 Закона о терроризме 2006 года, которая предоставляет полиции право направлять лицам, связанным с управлением вебсайтами или другими интернет-ресурсами, предписания об "удалении".

173. Действие статьи 3 Закона распространяется на дела, касающиеся правонарушений, предусмотренных в статьях 1 и 2 данного Закона, в связи с которыми "*a)* сообщение публикуется или организуется его публикация в ходе предоставления или использования услуг, предоставляемых в электронном виде либо в связи с ними; или *b)* поведение, подпадающее под действие пункта 2 статьи 2 [распространение публикаций террористического содержания], имело место в ходе предоставления или использования таких услуг или в связи с ними".

174. В пункте 2 статьи 3 предусматривается, что если лицо, которому было направлено соответствующее предписание, не удаляет связанный с терроризмом контент и если ему или ей впоследствии в связи с этим предъявляется обвинение в совершении правонарушений, предусмотренных в статьях 1 и 2 Закона о терроризме 2006 года, то в ходе судебного разбирательства может быть сделано опровержимое предположение, что информация, о которой идет речь, была опубликована с его или ее одобрения.

175. Несмотря на возможность использования предписаний об "удалении" в качестве предупредительной меры, на практике эти полномочия пока не использовались. В большинстве случаев, особенно когда противозаконный контент размещался на веб-сайтах третьих сторон, это, как правило, делалось в нарушение правил и условий провайдера услуг, и компетентным органам удавалось успешно договариваться об удалении противозаконной информации. В Соединенном Королевстве создано специализированное Информационное бюро по борьбе с терроризмом в Интернете, которое фактически осуществляет координацию предпринимаемых на национальном уровне, по запросам общественности, а также правительства и промышленных кругов, ответных мер в отношении содержимого Интернета, связанного с терроризмом, и выступает в качестве специализированного центрального источника рекомендаций для полицейской службы.

4. Международное сотрудничество

176. Согласно положениям ряда различных международных, региональных, многосторонних и двусторонних документов, касающихся борьбы с терроризмом и транснациональной организованной преступностью, государства обязаны разработать политику и создать законодательные основы для содействия налаживанию эффективного международного сотрудничества в расследовании и уголовном преследовании по делам такого рода.

177. В дополнение к политике и законодательству, которыми вводятся составы уголовных преступлений, необходимые для удовлетворения критериям "двойной уголовной ответственности", государства должны принять всеобъемлющее законодательство, которое обеспечит их компетентным органам правовую основу для международного сотрудничества с зарубежными

[109] Catherine A. Theohary and John Rollins, "Terrorist use of the Internet: information operations in cyberspace", Congressional Research Service report (8 March 2011), p. 8.

партнерами в расследовании дел, связанных с транснациональным терроризмом. В случаях, имеющих отношение к использованию Интернета, весьма вероятно, что эффективное международное сотрудничество, в том числе возможность обмениваться информацией, включая связанные с Интернетом данные, будет основным фактором в обеспечении успеха любого уголовного преследования.

178. Вопросы международного сотрудничества по делам, связанным с терроризмом, более подробно рассматриваются в главе V, ниже.

IV. Расследования и сбор оперативной информации

A. Инструментарий, используемый террористами при совершении преступлений, связанных с Интернетом

179. Технологический прогресс предоставляет в распоряжение террористов множество современных средств, с помощью которых они могут злонамеренно использовать Интернет в противозаконных целях. Для эффективного расследования деятельности, связанной с использованием Интернета, требуется сочетание традиционных методов ведения следствия, знание доступных инструментальных средств для осуществления незаконной деятельности через Интернет и разработка практических методик в целях выявления, задержания и судебного преследования виновных в совершении таких актов.

180. Одно из дел, слушавшихся во Франции, служит иллюстрацией того, как различные методы расследования, традиционные и специально ориентированные на работу с цифровыми уликами, применяются совместно в целях сбора доказательств, необходимых для успешного осуществления судебного преследования в связи с использованием Интернета террористами.

Государственный обвинитель против Арно, Бадаша, Гиаля и других

По данному делу, рассматривавшемуся во Франции, проходили несколько обвиняемых: Рани Арно, Надир Захир Бадаш, Адриан Лучиано Гиаль и Юссеф Лаабар, которые 26 января 2012 года были осуждены исправительным судом Парижа и приговорены к тюремному заключению на сроки от 18 месяцев до 6 лет, в том числе за распространение материалов, связанных с терроризмом.

Арно, Бадаш и Гиаль были арестованы во Франции в декабре 2008 года, после того как Арно, действовавший под именем пользователя Абдалла, поместил на пропагандистском веб-сайте minbar-sos.com сообщения с призывом к джихаду против Франции:

> Не забывайте, что Франция по-прежнему воюет с нашими братьями в Афганистане и что вы находитесь на территории войны; не теряйте времени, вступайте в ряды мучеников, бойкотируйте их экономику, разбазаривайте их богатства, не поддерживайте их экономику и не участвуйте в финансировании их армий.

Размещение данного сообщения позволило органам власти, перехватив учетную запись Арно в Интернете, установить за ним агентурное наблюдение и наладить прослушивание его телефонной линии. После ареста г-на Арно следователи провели судебную экспертизу контента используемых им компьютеров и установили, что он занимался изучением вопросов, касавшихся совершения террористических актов, в частности исследованием препаратов, которые можно использовать для изготовления взрывчатых веществ и зажигательных устройств, определением возможных целей и отслеживанием деятельности компании, использующей аммиачную селитру. Следствие показало, что Арно завербовал Гиаля и Бадаша, принимал участие в совещаниях и обсуждениях, касавшихся подготовки нападения, установил контакт с лицами, участвующими в джихадистском движении, чтобы заручиться их помощью в его осуществлении, и получил ряд денежных переводов на его финансирование. Эти деяния являлись преступлениями согласно статьям 421-2-1, 421-1, 421-5, 422-3, 422-6 и 422-7 Уголовного кодекса Франции, а также статьям 203 и 706-16 и далее Уголовно-процессуального кодекса.

Суд пришел к выводу, что план, в котором г-н Арно якобы принимал участие вместе с другими правонарушителями и согласно которому предполагалось подорвать размещенные на грузовике взрывчатые вещества по достижении им намеченной цели, представлял чрезвычайно серьезную угрозу для общественного порядка. Поэтому г-н Арно был приговорен к шести месяцам тюремного заключения по обвинениям, связанным с участием в группе, совершавшей преступные деяния в целях подготовки террористического акта, владением несколькими поддельными документами и незаконным использованием административных документов, подтверждавших право, личность или качество либо предоставлявших полномочия. По тому же обвинению г-н Бадаш был приговорен к двум годам лишения свободы, в том числе к шести месяцам условно, в то время как г-на Гиаля приговорили к четырем годам лишения свободы, включая один год условно. Г-н Лаабар, который предстал перед судом за другие связанные с этим деяния, был приговорен к 18 месяцам лишения свободы.

181. Для осуществления расследований и судебного преследования по делам, в которых фигурируют цифровые улики, необходимы специальные навыки ведения уголовных расследований, а также компетентность, знания и опыт, позволяющие применять эти навыки в виртуальной среде. Хотя допустимость доказательств в конечном счете является вопросом права и, следовательно, относится к компетенции прокуроров, следователи должны быть знакомы с правовыми и процедурными критериями установления степени допустимости в целях как внутренних, так и международных расследований. Основательное практическое знание требований применимых правил представления улик, и в частности в отношении цифровых улик, способствует сбору следователями достаточного количества допустимых доказательств для обеспечения успешного судебного преследования по делу. Например, процедуры, используемые при сборе, хранении и анализе цифровых улик, должны обеспечивать соблюдение четкого "режима охраны" со времени его первоначального установления, чтобы улики нельзя было фальсифицировать в период с момента их выемки до окончательного представления в суде[110].

1. Связь на основе интернет-технологий

a) Протокол передачи голоса через Интернет

182. За последнее десятилетие выросла популярность приложений, позволяющих пользователям общаться в реальном времени с помощью системы телефонии по протоколу передачи голоса через Интернет (VoIP), видеочата или текстового чата, и они стали более совершенными. В некоторых из этих приложений предусмотрены продвинутые функции по обмену информацией, например позволяющие пользователям совместно работать над файлами или дающие им возможность в реальном времени на удалении наблюдать за экранной деятельностью другого пользователя. Система VoIP, в частности, все чаще используется в качестве эффективного средства общения через Интернет. К числу широко известных провайдеров услуг системы VoIP относятся Skype и Vonage, работа которых основана на преобразовании аналогового звука в сжатый цифровой формат, что позволяет передавать через Интернет пакеты цифровой информации, используя соединения по относительно узкополосным каналам.

183. Поскольку система телефонии VoIP предполагает передачу пакетов цифровых данных, а не аналоговых сигналов, и поскольку провайдеры услуг, как правило, формируют выставляемые абонентам счета за пользование Интернетом исходя из совокупного объема данных,

[110] См., например, Association of Chief Police Officers (United Kingdom), *Good Practice Guide for Computer-Based Electronic Evidence*. См. по адресу: www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

счета за межкомпьютерные вызовы в системе VoIP не выставляются за каждый отдельный вызов, как это делается в традиционных системах мобильной и фиксированной телефонной связи. Такое различие в практике выставления счетов может существенно воздействовать на ход расследований, касающихся обменов сообщениями с использованием системы VoIP, так как при этом правоохранительным органам труднее подтвердить такие обмены маркерами, указывающими, например, на время вызова и местонахождение участников. Однако в качестве средств для установления личности виновных в противозаконной деятельности в Интернете могут также служить другие показатели, такие как время передачи и объем трафика данных в Интернете (см. пункт 205, ниже). Кроме того, в то время как источник и адрес назначения обычных телефонных звонков можно проследить через коммутаторы стационарных линий или антенные мачты сотовой связи, где остаются следы геолокации, обмены сообщениями, осуществляемые с помощью целиком основанной на интернет-технологиях системы VoIP, например через беспроводные сети, могут создавать проблемы для ведущих расследование. Дополнительными осложняющими факторами, связанными с использованием технологии VoIP, могут стать в том числе маршрутизация вызовов через одноранговые сети и шифрование адресов вызова (более подробно см. в разделе A.2 главы IV, ниже)[111].

184. Однако должным образом оформленные запросы к провайдерам услуг VoIP о предоставлении информации все-таки могут обеспечить получение полезных идентифицирующих данных, таких как IP-адрес пользователя, адрес его электронной почты или платежные реквизиты.

b) Электронная почта

185. Службы электронной почты на базе интернет-технологий также предоставляют в распоряжение террористов средство скрытого обмена сообщениями, которое может быть злонамеренно использовано в противозаконных целях. Сообщения электронной почты, отправляемые сторонами друг другу, как правило, содержат ряд элементов, которые могут быть полезны для следствия. Типичное письмо электронной почты может состоять из заголовка конверта, заголовка сообщения, тела сообщения и любых связанных с ним вложений. Хотя в зависимости от настроек применяемого программного обеспечения отображаться может лишь сокращенный вариант заголовка конверта, полный заголовок конверта обычно содержит сведения о каждом почтовом сервере, через который сообщение проходило на пути к конечному адресату, а также информацию об IP-адресе отправителя[112]. Информация, содержащаяся в заголовке конверта, менее подвержена фальсификации (хотя и не застрахована от нее), чем информация в заголовках сообщений, которая обычно состоит из сведений, предоставляемых пользователем, в таких полях, как "Кому", "От кого", "Обратный путь", "Дата" и "Время", фигурирующих на устройстве, с которого отправляется сообщение[113].

186. Одним из часто используемых методов для сокращения количества остающихся между сторонами электронных следов и, следовательно, вероятности обнаружения является поддержание связи путем сохранения неотправленных сообщений в папке черновиков учетной записи абонента электронной почты. Тогда эта информация становится доступной ряду лиц, использующих для доступа к этой учетной записи общий пароль. В целях избежания обнаружения могут также приниматься дополнительные меры, такие как использование для доступа к соответствующим проектам сообщений общественных терминалов удаленного доступа, например в интернет-кафе. Данный метод был использован в связи со взрывами бомб террористами в Мадриде в 2004 году.

---

[111] Письменный материал, представленный экспертом из Группы специального назначения Корпуса карабинеров Италии.

[112] United States, Department of Justice, Office of Justice Programs, National Institute of Justice, *Investigations Involving the Internet and Computer Networks* (2007), p. 18 ff.

[113] Ibid., p. 20.

187. Кроме того, при передаче сообщений по электронной почте могут использоваться методы анонимизации (более подробно см. в разделе A.2 главы IV, ниже), например маскирующие IP-адрес, принадлежащий отправителю электронной почты. Могут также использоваться анонимные почтовые серверы, которые удаляют идентифицирующую информацию из заголовка конверта, прежде чем переслать его на последующий почтовый сервер.

Важность международного сотрудничества в расследовании деятельности в Интернете, связанной с терроризмом

Эксперт из Группы специального назначения Корпуса карабинеров Италии обрисовал ключевую роль международного сотрудничества и специальных методов ведения следствия в расследовании случая использования Интернета в террористических целях базирующейся в Турции экстремистской организацией "Революционная народно-освободительная партия/фронт" (РНОП/Ф). Тесное взаимодействие между сотрудниками правоохранительных органов Турции и Италии позволило итальянским следователям установить, какие методы шифрования и другие меры защиты данных применялись членами РНОП/Ф в рамках обмена информацией для содействия достижению террористических целей, включая использование онлайновых служб электронной почты. В частности, члены РНОП/Ф использовали программу стенографирования "Камуфляж" для сокрытия информации в графических файлах в форматах JPEG и GIF и программу WinZip для шифрования файлов, прилагаемых в виде вложений к сообщениям электронной почты (см. раздел A.2 главы IV, ниже). Итальянские следователи перехватили или иными способами получили доступ к паролям шифрования и определили соответствующие программы, что помогло декодировать сообщения. Дополнительная информация была получена благодаря проведению судебной экспертизы компьютеров с использованием программы EnCase (см. раздел C главы IV, ниже), а также применению традиционных методов расследования, позволявших следователям получать цифровые улики с компьютеров подозреваемых, находившихся под следствием. Результаты этого расследования, наряду с широким трансграничным сотрудничеством, привели к аресту в апреле 2004 года 82 подозреваемых в Турции и еще 59 подозреваемых в Бельгии, Германии, Греции, Италии и Нидерландах.

c) Онлайновые службы обмена сообщениями и дискуссионные форумы

188. Онлайновые службы доставки и отправления сообщений и дискуссионные форумы являются дополнительным средством обмена сообщениями в реальном времени с различной степенью потенциальной анонимности. Онлайновые службы обмена сообщениями обычно позволяют поддерживать двустороннюю связь, тогда как дискуссионные форумы обеспечивают свободное общение между группами лиц. Регистрация в онлайновых службах обмена сообщениями, как правило, осуществляется на основе непроверенной информации, предоставленной пользователем; однако отдельные интернет-службы также фиксируют использовавшиеся при регистрации IP-адреса, которые могут быть затребованы правоохранительными органами на условиях соблюдения применимых правовых гарантий. Сообщения обычно идентифицируются по уникальному псевдониму, который может назначаться на постоянной основе при регистрации или ограничиваться использованием в ходе конкретного сеанса работы в Интернете. Провайдеры услуг, как правило, не записывают информацию, которой стороны обмениваются во время сеанса работы в онлайновых службах обмена сообщениями, и, следовательно, по завершении сеанса работы в Интернете эта информация может оказаться недоступной для извлечения, а для ее восстановления потребуется прибегнуть к судебной экспертизе жесткого диска одного из участников.

189. Для того чтобы способствовать развитию чувства общности в мировом масштабе, террористические организации и сочувствующие им могут использовать защищенные паролем

дискуссионные форумы. Публикуемые в дискуссионных форумах сообщения могут быть подвержены более тщательному мониторингу и учету со стороны провайдеров услуг, чем двусторонние обмены сообщениями, что повышает потенциальную вероятность получения документальных доказательств в ходе расследований[114]. В ряде юрисдикций сотрудникам правоохранительных органов в связи с проведением расследования разрешается, на определенных условиях, тайно зарегистрироваться и участвовать под псевдонимом в обсуждениях, которые ведутся в дискуссионных группах.

190. Например, во Франции статьей 706 Уголовно-процессуального кодекса предусматривается, что для проведения таких операций по инфильтрации в связи с преступлениями, совершаемыми с использованием электронных средств связи, требуется санкция прокурора или судьи, ведущего судебное следствие (см. обсуждение в разделе C.3 *a)* главы III). Целью таких операций может быть, в частности, сбор информации или проведение других предупредительных мероприятий в связи с предполагаемой террористической угрозой. Однако, приступая к проведению операции, необходимо уделить должное внимание гарантиям того, что любое проникновение в онлайновый дискуссионный форум или другие дискуссионные группы в Интернете будет осуществлено таким образом, чтобы оно не могло быть использовано для защиты ссылкой на провокацию со стороны представителей правоприменяющих органов, основанной на утверждении, будто сотрудники государственного учреждения вынудили подозреваемого совершить уголовно наказуемое деяние, к совершению которого он или она не были изначально предрасположены.

d) Файлообменные сети и "облачные" технологии

191. Файлообменные сайты, такие как Rapidshare, Dropbox или Fileshare, дают сторонам возможность без труда загружать, делиться, находить и получать доступ к мультимедийным файлам через Интернет. Методы шифрования и анонимизации, используемые в связи с другими формами интернет-связи, в той же мере применимы к файлам, обмен которыми осуществляется с помощью в том числе пиринговых технологий (P2P) и протокола передачи файлов (FTP). Например, по делу Ишора (см. пункт 20, выше) были представлены доказательства того, что обмен цифровыми файлами в поддержку террористической деятельности, после их шифрования и архивации в целях обеспечения безопасности, осуществлялся через Rapidshare. Некоторые файлообменные сети могут вести журналы передачи данных или сохранять информацию о платежах, которые могут представлять интерес в контексте расследования.

192. "Облачные" вычисления – это сервис, который предоставляет пользователям удаленный доступ к программам и данным, хранящимся или выполняемым на серверах данных, принадлежащих третьим сторонам. Как и обмен файлами, "облачные" вычисления представляют собой удобное средство для безопасного хранения, обмена и распространения материалов в Интернете. Использование "облачных" технологий для доступа к информации, хранимой на удаленных носителях, помогает сократить объем данных, хранящихся локально на отдельных устройствах, и, соответственно, уменьшить возможности получения потенциальных доказательств в связи с расследованиями, касающимися использования Интернета в террористических целях.

193. Серверы данных, используемые для оказания этих услуг, также могут физически находиться в иной юрисдикции, нежели зарегистрированный пользователь, с иными уровнями регулирования и возможностями правоприменения. Поэтому для получения ключевых улик в целях проведения судебного разбирательства может быть необходима тесная координация с местными правоохранительными органами.

[114] Ibid., pp. 34 ff.

2. Методы шифрования данных и сохранения анонимности

194. Шифрованием данных называется защита цифровой информации от раскрытия путем преобразования ее в криптограмму с использованием математических алгоритмов и ключа шифрования, чтобы она была понятна только намеченному получателю. Средства шифрования могут быть реализованы на аппаратной или программной основе или на основе сочетания того и другого. После шифрования для получения доступа к информации могут потребоваться пароль, фраза-пароль, "программный ключ" или аппаратное средство доступа либо определенное их сочетание. Шифрование может применяться в отношении данных "в состоянии покоя", содержащихся в памяти таких устройств, как жесткие диски компьютеров, флеш-память и смартфоны, а также в отношении данных "в пути", передаваемых через Интернет, например с помощью VoIP-телефонии и сообщений электронной почты. К числу примеров распространенных программных средств шифрования можно отнести службы, интегрированные в компьютерные операционные системы или прикладные программы, а также такие автономные программы, как Pretty Good Privacy и WinZip[115]. В рамках дела, слушавшегося в Бразилии, на основе международного сотрудничества и обмена информацией было начато расследование в отношении подозреваемого, которого обвиняли в том, что он участвовал в деятельности джихадистского веб-сайта, связанного с признанной террористической организацией, а именно с "Аль-Каидой", выступал там в качестве модератора и контролировал эту деятельность. На этом веб-сайте размещались видеоматериалы, тексты и обращения боевиков-экстремистов руководящего уровня в переводе на английский язык, чтобы охватить более широкую аудиторию; он также использовался для проведения акций по сбору средств и пропагандистских кампаний расистской направленности. Полицейская операция, которая привела к задержанию этого подозреваемого, имела целью захватить его врасплох, когда он был подключен к Интернету и активно занимался деятельностью, связанной с веб-сайтом. Задержав подозреваемого в момент, когда его компьютер был включен и соответствующие файлы были открыты, следователи смогли обойтись без симметричных криптографических ключей и других средств шифрования и обеспечения безопасности, использовавшихся подозреваемым и его сообщниками. Таким образом следователям удалось получить доступ к цифровому контенту, который в противном случае мог бы оказаться недоступным, или им было бы труднее овладеть, если бы компьютер был выключен и защищен.

195. Сокрытие деятельности в Интернете или личности причастных к ней пользователей также может осуществляться с помощью передовых технологий, включая маскирование IP-адреса источника, ложное представление под IP-адресом другой системы или перенаправление интернет-трафика на скрытый IP-адрес[116]. Прокси-серверы позволяют пользователям скрытно выполнять косвенные запросы к другим сетевым службам. Некоторые прокси-серверы позволяют сконфигурировать браузер пользователя таким образом, чтобы трафик браузера автоматически направлялся через прокси-сервер. Прокси-сервер отправляет запросы на сетевые услуги от имени пользователя, а затем задает маршрут доставки результатов снова через прокси-сервер. Использование прокси-серверов может способствовать достижению тех или иных уровней анонимности. Прокси-сервер способен скрыть личность пользователя, выполняя запросы на сетевые услуги без раскрытия IP-адреса, с которого исходит запрос, или намеренно предоставляя искаженный IP-адрес источника. Например, такие прикладные программы, как The Onion Router, могут использоваться в целях защиты анонимности пользователей путем автоматического перенаправления деятельности в Интернете через сеть прокси-серверов, для того чтобы замаскировать ее первоначальный источник. Перенаправление сетевого трафика через несколько прокси-серверов, потенциально находящихся в разных юрисдикциях, повышает степень трудности точного установления отправителя исходящих сообщений.

[115] United States, Department of Justice, Office of Justice Programs, National Institute of Justice, *Investigative Uses of Technology: Devices, Tools and Techniques* (2007), p. 50.

[116] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, p. 9.

196. В качестве альтернативы подозреваемый может взломать IP-адрес законной организации и просматривать информацию в Интернете, используя взломанный адрес. Любые следы такой деятельности были бы связаны с IP-адресом пострадавшей организации. Через взломанный компьютер подозреваемый также может получать доступ к тем или иным веб-сайтам или хранить на взломанных веб-сайтах вредоносные программы (используемые, например, для получения сведений о кредитных картах или другой личной финансовой информации) в целях избежания опознания.

197. Существует множество компьютерных программ, которые могут использоваться для сокрытия или шифрования данных, передаваемых через Интернет в противозаконных целях. Эти программы могут включать использование такого программного обеспечения, как "Камуфляж", для маскировки информации с помощью стеганографии или шифрование и парольную защиту файлов с помощью такого программного обеспечения, как WinZip. Может также использоваться многоуровневая защита данных. Например, программа "Камуфляж" позволяет скрывать файлы путем их скремблирования и последующего прикрепления в конце файла-носителя по своему выбору. Файл-носитель сохраняет свои первоначальные свойства, но используется в качестве носителя для хранения или передачи скрытого файла. Данное программное обеспечение может применяться к широкому диапазону типов файлов. Скрытый файл, однако, можно обнаружить путем анализа первичных данных файла, который покажет наличие прикрепленного скрытого файла[117].

198. В Соединенном Королевстве, согласно Закону о регулировании полномочий следственных органов 2000 года, отказ выполнить требование о передаче ключа шифрования рассматривается как уголовно наказуемое преступление. Однако необходимо заботиться о том, чтобы предупредить попытки подозреваемых уклониться от действия данного положения путем использования нескольких уровней шифрования и нескольких ключей для защиты различных массивов данных. Например, в программе TruCrypt, являющейся одним из популярных бесплатных средств шифрования, имеется установка, позволяющая подозреваемому при шифровании жесткого диска создать два пароля: один – для "чистой" части диска, а другой – для части, содержащей инкриминирующие материалы. Обойти это можно, если обеспечить, чтобы при проведении судебной экспертизы жесткого диска осуществлялась проверка на наличие "недостающих томов" информации. Кроме того, правонарушения такого рода, как правило, относятся к категории преступлений, преследуемых в порядке суммарного производства, максимальным наказанием за которые является лишение свободы сроком на шесть месяцев. Однако в Соединенном Королевстве, когда дело касается вопросов национальной безопасности, максимальный срок наказания увеличивается до двух лет лишения свободы.

3. Беспроводные технологии

199. Беспроводные сетевые технологии позволяют компьютерам и другим устройствам получать доступ в Интернет с помощью радиосигналов, а не через постоянное соединение, например по кабелю. Чтобы получить доступ к сети Wi-Fi, необходимо находиться на относительно небольшом расстоянии от сетевых ресурсов, которое зависит от силы беспроводного сигнала. Беспроводные сети могут быть сконфигурированы таким образом, чтобы позволялся открытый доступ в Интернет без регистрации, или же они могут быть защищены с использованием парольной фразы или различных уровней шифрования. Доступ к беспроводным сетям, зарегистрированным на физических лиц, предприятия или государственные структуры, нередко можно получить из общественных мест. Анонимный доступ к защищенным или незащищенным сетям Wi-Fi может позволять преступникам скрывать связь между их деятельностью в Интернете и идентифицирующей информацией.

[117] Письменный материал, представленный экспертом из Группы специального назначения Корпуса карабинеров Италии.

200. Кроме того, в последние годы появился ряд провайдеров услуг, таких как Fon, которые позволяют зарегистрированным пользователям делиться частью пропускной способности своих домашних каналов связи Wi-Fi с другими абонентами в обмен на взаимный доступ к сетям Wi-Fi абонентов по всему миру. В ходе расследования осуществление деятельности в коллективно используемых сетях Wi-Fi существенно затрудняет процесс установления причастности к совершению того или иного деяния единственного правонарушителя, который может быть идентифицирован[118].

201. Один из нестандартных методов связан с использованием программно определяемых высокочастотных (ВЧ) радиоприемников с улучшенными рабочими характеристиками, конфигурируемых через компьютер. Таким образом не происходит обмена данными через сервер и не создается никаких журналов регистрации. Правоохранительным и разведывательным органам сложнее перехватывать сообщения, отправляемые с использованием данного метода как в плане установления местонахождения передатчиков, так и в плане предсказания в реальном времени частоты, на которой передаются сообщения.

B. Расследование дел о терроризме, связанных с использованием Интернета

1. Систематический подход к расследованиям, связанным с использованием Интернета

202. Существует широкий спектр доступных через Интернет данных и услуг, которые могут использоваться при проведении расследований, направленных на противодействие использованию Интернета террористами. Основанный на использовании развивающихся интернет-ресурсов проактивный подход к стратегиям проведения расследований и специализированным вспомогательным средствам способствует эффективному выявлению данных и услуг, способных принести максимальную пользу следствию. Признавая необходимость систематического подхода к использованию в целях проведения расследований технологических разработок, связанных с Интернетом, Группа специального назначения Корпуса карабинеров Италии выработала руководящие принципы, которые были распространены через программу магистратуры университетского колледжа Дублина в области судебной экспертизы с применением компьютеров и борьбы с киберпреступностью (см. раздел G главы IV, ниже) и реализованы национальными правоприменительными органами многих государств – членов Международной организации уголовной полиции (Интерпол) и Европейского полицейского управления (Европол).

Протокол систематического подхода

- *Сбор данных*. Этот этап предполагает сбор с помощью традиционных методов ведения следствия такой информации, как сведения, касающиеся подозреваемого, любых лиц, проживающих вместе с ним, его имеющих отношение к делу сотрудников или иных партнеров, а также собираемые с помощью обычных методов слежения сведения об используемых каналах связи, в том числе о пользовании стационарными и мобильными телефонными линиями.

[118] Там же.

- *Поиск дополнительной информации, доступной через сервисы, основанные на интернет-технологиях*. Этот этап предполагает рассылку запросов в целях получения информации, собираемой и хранимой в базах данных использующих интернет-технологии служб электронной торговли, связи и сетевых сервисов, таких как eBay, PayPal, Google и Facebook, а также использование специализированных поисковых механизмов, таких как www.123people.com. Данные, собираемые этими службами благодаря широкому использованию интернет-куки, позволяют также получить важные сведения об использовании несколькими пользователями одного компьютера или мобильного устройства.
- Проводимые на указанных выше этапах *a)* и *b)* мероприятия помогают получить информацию, которую можно обобщить и снабдить перекрестными ссылками в целях создания краткой характеристики подследственного или группы подследственных и предоставить для проведения анализа на более поздних этапах расследования.
- *Запросы к серверам VoIP*. На этом этапе правоохранительные органы запрашивают у провайдеров услуг VoIP информацию, касающуюся подследственных и любых других известных лиц, причастных к совершению преступления, или пользователей тех же сетевых устройств. Собранная на этом этапе информация может также использоваться в качестве своего рода "умного фильтра" в целях проверки сведений, полученных на двух предыдущих этапах.
- *Анализ*. Большие объемы данных, полученных от серверов VoIP и провайдеров различных интернет-услуг, затем подвергаются анализу для выявления информации и тенденций, полезных в целях следствия. Содействовать проведению этого анализа могут компьютерные программы, позволяющие фильтровать информацию или представлять собранные цифровые данные в графическом виде, чтобы, в частности, высветить тенденции, хронологию, существование организованной группы или ее иерархическую структуру, географическое местоположение членов такой группы или факторы, общие для коллективных пользователей, такие как общие источники финансирования.
- *Выявление субъектов, представляющих интерес*. На этом этапе, после интеллектуального анализа данных, обычно выявляют, какие из субъектов могут представлять интерес, на основе, например, сведений об абонентах, связанных с их финансовыми счетами и учетными записями VoIP или электронной почты.
- *Мероприятия по перехвату*. На этом этапе правоохранительные органы применяют тактику перехвата, схожую с используемой применительно к традиционным каналам связи, перенеся ее на другую платформу: цифровые каналы связи. Мероприятия по перехвату могут осуществляться в отношении таких телекоммуникационных служб, как средства широкополосной стационарной, широкополосной мобильной и беспроводной связи, а также в отношении услуг, предоставляемых провайдерами доступа в Интернет, таких как электронная почта, дискуссионные группы и форумы. В частности, за последние годы были на опыте выявлены уязвимые места новых коммуникационных технологий, которые могут быть использованы в целях проведения расследований и сбора разведывательной информации. Должное внимание надлежит уделять сохранению до суда неприкосновенности собранных данных и подтверждению, насколько это возможно, любой собранной разведывательной информации такими объективными идентификаторами, как координаты системы GPS, временные метки или записи видеонаблюдения.

Там, где это допускается внутренним законодательством, некоторые правоохранительные органы могут также использовать цифровые методы слежения с помощью установки на компьютер подследственного аппаратных средств или приложений, таких как вирусы, "троянские кони" или клавиатурные шпионы. Этого можно достичь, получив прямой или удаленный доступ к соответствующему компьютеру с учетом технических характеристик аппаратных средств, которые предстоит взломать (например, наличия антивирусной защиты и брандмауэров), и личностных профилей всех пользователей соответствующего устройства, чтобы сориентироваться на пользователя с наименее продвинутым профилем.

203. Корейское национальное управление полиции, откликаясь на необходимость стандартизации внутренней правоприменительной практики, связанной с проведением судебной экспертизы с использованием цифровых устройств, разработало и внедрило два пособия: "Стандартные правила обращения с цифровыми уликами" и "Техническое руководство по цифровым методам судебной экспертизы". В Стандартных правилах подробно описаны семь этапов надлежащей обработки цифровых улик: подготовка, сбор, изучение, запросы о передаче улик, получение и транспортировка, анализ, подготовка отчетов, а также сохранение улик и распоряжение ими. В Техническом руководстве по цифровым методам судебной экспертизы описываются необходимые процедуры и надлежащие методы сбора цифровых улик, в том числе касающиеся создания подходящих условий и выбора средств и оборудования для проведения судебной экспертизы; подготовительные шаги, такие как настройка аппаратных средств и программного обеспечения, установление сетевых соединений и точный контроль времени; меры по обеспечению получения максимального количества цифровых данных; независимый анализ собранных данных; а также подготовка итогового отчета[119].

2. Отслеживание IP-адресов

204. Связанный с размещенным в Интернете сообщением IP-адрес является важным идентификатором и, соответственно, ключом к расследованию случаев использования Интернета террористами. IP-адрес служит для обозначения конкретной сети и устройства, используемых для доступа в Интернет. IP-адреса могут быть динамическими, временно назначаемыми на период сеанса работы в сети из пула адресов, доступных провайдеру услуг Интернет, или статическими (назначаемыми на постоянной основе, как в случае адресов веб-сайтов). Динамические IP-адреса обычно предоставляются провайдерам услуг Интернет из региональных блоков. Поэтому при отсутствии помех, вызываемых использованием средств анонимизации или других методов, динамический IP-адрес нередко может быть использован, чтобы установить, из какого региона или государства компьютер подключен к Интернету.

205. Кроме того, в ответ на надлежащим образом сделанный запрос провайдер услуг Интернет нередко может установить, какая из учетных записей его абонентов была связана с тем или иным IP-адресом в определенное время. После этого можно, пользуясь традиционными методами ведения следствия, выявить лицо, физически контролировавшее учетную запись данного абонента в указанное время. В деле *Ишора* (см. пункт 20, выше) обвиняемый был идентифицирован путем отслеживания статического IP-адреса, использовавшегося для доступа к учетной записи электронной почты, которая находилась под наблюдением. Обращенный к соответствующему провайдеру услуг Интернет запрос позволил компетентным органам связать этот IP-адрес с абонентским счетом, использовавшимся несколькими обитателями одного дома, в том числе обвиняемым. Перехватив связанный с этим абонентским счетом трафик данных, следователи также сумели выявить связи между данным IP-адресом и деятельностью проджихадистского веб-сайта, использовавшегося в том числе для распространения материалов по физической и психологической подготовке боевиков-экстремистов. В частности, следователям удалось установить наличие взаимосвязи между периодами массовых подключений к дискуссионному форуму на этом сайте с одновременным увеличением объемов передач через Интернет данных, связанных с учетной записью личной электронной почты обвиняемого[120].

206. Учитывая срочный характер расследований, касающихся Интернета, и существование риска того, что цифровые данные могут быть изменены или удалены, в частности из-за вероятных ограничений мощности сервера соответствующего провайдера услуг Интернет или

[119] Письменный материал, представленный экспертом из Республики Корея.

[120] Judgement of 4 May 2012, Case No. 0926639036 of the Tribunal de Grande Instance de Paris (14th Chamber/2), p. 7 et. seq.

в силу применимых правил о защите данных, внимание надлежит также уделять вопросу о целесообразности предъявления такому провайдеру услуг требования сохранять имеющие отношение к уголовному расследованию данные до тех пор, пока не будут приняты необходимые меры по защите этих данных для целей доказывания.

207. В случае если расследование касается веб-сайта, сначала необходимо преобразовать соответствующее доменное имя в IP-адрес. В целях установления соответствующего IP-адреса, который, в свою очередь, зарегистрирован в Корпорации по присвоению имен и номеров в Интернете (ICANN), можно использовать несколько специальных утилит. В число доступных через Интернет популярных утилит входят whois и nslookup[121]. Например, запрос через whois в отношении доменного имени Управления Организации Объединенных Наций по наркотикам и преступности (www.unodc.org) дает следующий результат:

Идентификатор домена: D91116542-LROR

Доменное имя: UNODC.ORG

Создан: 11 октября 2002 года; 09:23:23 ВСВ

Последнее обновление: 19 октября 2004 года; 00:49:30 ВСВ

Срок действия: 11 октября 2012 года; 09:23:23 ВСВ

Регистратор-поручитель: Network Solutions LLC (R63-LROR)

Статус: СМЕНА КЛИЕНТА ЗАПРЕЩЕНА

Идентификатор регистранта: 15108436-NSI

Имя регистранта: Висснер Александр

Организация регистранта: Организация Объединенных Наций, Вена

Уличный адрес регистранта: Vienna International Centre, P.O. Box 500

Город регистранта: A-1400 Wien (Вена) AT 1400

Почтовый индекс регистранта: 99999

Страна регистранта: AT

Номер телефона регистранта: +43.1260604409

Номер факса регистранта: +43.1213464409

Электронная почта регистранта: noc@unvienna.org

Эти сведения, однако, предоставляет сам регистрант. Вследствие этого, возможно, потребуются дополнительные шаги для самостоятельной проверки точности информации о регистранте. Кроме того, домены могут быть сданы в аренду или иным образом переданы под контроль лица, не являющегося регистрантом.

208. Лица, проводящие расследования по делам об использовании Интернета в террористических целях, должны также сознавать, что связанная с расследованием деятельность в Интернете может стать предметом мониторинга, записи и отслеживания со стороны третьих лиц. Поэтому им следует проявлять должную осторожность и избегать рассылки запросов через Интернет с устройств, которые можно проследить обратно к организации, ведущей расследование[122].

[121] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, p. 10.

[122] Ibid.

3. Доступные следственным органам специализированные утилиты и аппаратные средства

209. В распоряжении следователей, обладающих соответствующими техническими знаниями, имеется ряд специализированных утилит и аппаратных средств. Некоторые из них, такие как Ping и Traceroute, могут быть интегрированы в операционную систему устройства, являющегося объектом расследования. Ping, например, можно использовать для передачи сигнала на компьютер, имеющий подключение к Интернету, чтобы установить, подключен ли он в данный момент, хотя это зависит от наличия помех, создаваемых какими-либо брандмауэрами или иными особенностями конфигурации сети. Аналогичным образом, с помощью Traceroute можно определить маршрут между двумя компьютерами, объединенными в сеть, что может способствовать установлению их физического местонахождения.

210. К числу других программ, которые могут использоваться, если это не запрещено внутренними законами и правилами в отношении, в частности, получения доступа к устройству и перехвата сообщений, относятся программы типа "троянский конь" или трояны, реализующие удаленное администрирование, которые можно тайно внедрить в компьютерную систему для сбора информации или установления дистанционного управления скомпрометированной машиной. На устройство также можно установить средства мониторинга нажатия клавиш на клавиатуре и использовать их для мониторинга и записи действий на клавиатуре. Клавиатурные шпионы в аппаратном или программном исполнении помогают получить информацию, касающуюся, в частности, паролей, обменов сообщениями и посещаемых веб-сайтов или деятельности, осуществляемой локально с помощью подконтрольного устройства. Кроме того, для сбора данных, имеющих отношение к расследованию, могут использоваться сетевые анализаторы пакетов данных. "Снифферы", которые могут быть выполнены в виде устройства или программного обеспечения, ведут сбор информации непосредственно в сети, и с их помощью можно получать сведения об источнике и контенте сообщений, а также о передаваемом контенте.

C. Сохранение и восстановление данных в рамках криминалистической экспертизы

211. Важная часть работы по добыче улик в делах, связанных с использованием Интернета в террористических целях, состоит в восстановлении хранимых цифровых данных. Двумя основными задачами таких мероприятий по восстановлению данных являются поиск значимых улик в целях обеспечения успешного завершения следствия и судебного преследования и сохранение целостности источника данных и режима их охраны, чтобы гарантировать их допустимость в процессе судопроизводства. Для определения наилучшего способа сохранения доказательств важно проводить различие между непостоянной информацией, которая хранится в устройствах, например в запоминающем устройстве с произвольной выборкой (RAM), и может быть безвозвратно утрачена в случае нарушения энергоснабжения, и энергонезависимой информацией, которая сохраняется независимо от энергоснабжения устройства. Например, акт отключения компьютера может привести к изменению хранящейся в запоминающих устройствах и оперативной памяти информации, которая может содержать важные улики, относящиеся к используемым подозреваемым компьютерным программам или посещаемым им веб-сайтам. Непостоянные данные могут содержать сведения о текущих процессах на работающем компьютере, которые могут быть полезны для следствия, таких как информация, касающаяся пользователей, паролей, незашифрованных данных или мгновенных сообщений. Примерами устройств хранения энергонезависимой информации являются внутренние/внешние жесткие диски, портативные дисковые накопители, устройства флеш-памяти и zip-дисководы.

212. Департамент национальной безопасности Соединенных Штатов представил полезный обзор данного процесса в руководстве под названием "Передовой опыт выемки улик

в электронной форме: карманный справочник для специалистов оперативного реагирования"[123]. В этом руководстве описываются следующие меры по сохранению доказательств в связи с уголовными расследованиями, касающимися использования вычислительных устройств.

Наилучшие методы сохранения данных

- Не пользуйтесь компьютером и не пытайтесь искать улики.
- Если компьютер подключен к сети, выньте из розетки вилку источника питания маршрутизатора или модема.
- Прежде чем перемещать какие-либо вещественные доказательства, сфотографируйте компьютер в том виде, в каком он был обнаружен, включая вид спереди и вид сзади, а также любые кабели или присоединенные устройства и окружающее пространство.
- Если компьютер выключен, не включайте его.
- Если компьютер включен и на мониторе имеется какое-либо изображение, сфотографируйте его экран.
- Если компьютер включен, а экран погашен, сделайте движение мышью или нажмите на клавишу пробела (в результате на экране появится активное изображение); после того как появится изображение, сфотографируйте экран.
- Для настольных компьютеров: выньте шнур питания из розетки на задней стороне корпуса компьютера.
- Для портативных компьютеров: отсоедините кабель питания; если ноутбук не выключается, найдите и удалите аккумуляторную батарею (батарея обычно помещается на дне, и там, как правило, имеется кнопка или переключатель, позволяющие ее удалить); после того как батарея будет удалена, не возвращайте ее на место и не храните внутри ноутбука (это позволит избежать случайного включения компьютера).
- Нарисуйте схему кабельных подключений и пометьте кабели, чтобы позднее опознать присоединенные устройства.
- Отсоедините все кабели и устройства от настольного компьютера или ноутбука.
- Упакуйте и перевозите все компоненты (включая маршрутизатор и модем, если таковые имеются) как хрупкий груз.
- Если это допускается по условиям любого применимого ордера на обыск, произведите выемку любых дополнительных носителей информации.
- Не храните никакие носители, включая корпус ПК, вблизи магнитов, радиопередатчиков и других предметов, потенциально способных их повредить.
- Соберите инструкции по эксплуатации, документацию и заметки, уделяя особое внимание любым предметам, которые могут помочь выяснить относящиеся к компьютеру пароли или фразы-пароли.
- Задокументируйте все шаги, связанные с изъятием компьютера и его компонентов.

213. Что касается мобильных устройств, таких как смартфоны и персональные цифровые помощники, то в их отношении применяются аналогичные принципы за тем исключением, что не рекомендуется отключать питание устройства, поскольку это может привести к активации защиты паролем и, таким образом, перекрыть доступ к уликам. Поэтому такое

[123] United States, Department of Homeland Security, "Best practices for seizing electronic evidence: a pocket guide for first responders", 3rd ed. (2007). См. по адресу: www.forwardedge2.com/pdf/bestPractices.pdf.

устройство следует, насколько это возможно, держать заряженным или как можно скорее, прежде чем батарея разрядится, подвергнуть специальному анализу, чтобы избежать потери данных.

214. Приведенное ниже дело, слушавшееся в Индии, подтверждает важность криминалистической экспертизы для выявления и восстановления цифровых и других доказательств использования Интернета террористами.

Дело Зия Уль Хака

Обвиняемый Зия Уль Хак, арестованный 3 мая 2010 года и в настоящее время ожидающий суда, подозревается в том, что он является членом "Лашкаре-Тайба", которая представляет собой базирующуюся в Пакистане вооруженную группу, ведущую борьбу против контроля Индии над Кашмиром. В деле против Зия Уль Хака обвинение утверждает, в частности, что его привлекли к участию в джихаде в период работы в Саудовской Аравии в 1999–2001 годах; находясь за пределами Индии, он прошел обучение пользованию оружием, подрывными средствами и взрывчатыми веществами и поддержанию связи через электронную почту; в 2005 году, по поступлении соответствующего поручения по электронной почте, он получил в Дели партию оружия, боеприпасов и взрывчатых веществ; а впоследствии он использовал Интернет для координации действий с другими членами группы "Лашкаре-Тайба" и вступил в сговор в целях совершения террористических актов с использованием оружия, боеприпасов и взрывчатых веществ.

Обвинение утверждает, кроме того, что 7 мая 2006 года Зия Уль Хак применил ручные гранаты, поставленные с полученной от "Лашкаре-Тайба" партией оружия, при нападении на кинотеатр "Одеон" в Хайдарабаде.

От провайдеров услуг Интернет были получены электронные письма, которыми обвиняемый обменивался со своим куратором, и было исследовано их содержание. Судебной экспертизе были подвергнуты компьютеры в интернет-кафе, которыми пользовался обвиняемый. Также удалось проследить, в каком отеле он останавливался, находясь в Дели, чтобы получить гранаты, и судебная экспертиза подтвердила подлинность его подписи в книге записи постояльцев. Пока обвиняемый находился в тюрьме в ожидании суда, из Индии в адрес центрального органа другой страны было направлено судебное поручение с просьбой возбудить дело против предполагаемого куратора.

Зия Уль Хак был обвинен в Индии в совершении ряда преступлений, в том числе по статьям 15, 16, 17 и 18 Закона 1967 года о (пресечении) противоправной деятельности с поправками, внесенными в него в 2004 и 2008 годах, которыми предусматривается наказание за террористическую деятельность, обучение и вербовку в террористических целях, сбор средств на ведение террористической деятельности и сговор в целях совершения террористических актов.

215. В силу того что цифровые улики легко повредить, наиболее эффективно их оценку, сбор и исследование способны выполнить специально подготовленные судебные эксперты. Во внутреннем законодательстве Израиля признается значение специальной подготовки и предусматривается, что сбор цифровых улик должен осуществляться квалифицированными следователями по компьютерам, которые проходят базовый курс профессиональной подготовки, а затем повышают свою квалификацию по месту работы, знакомясь с компьютерными системами и разного рода компьютерными программами в целях проведения криминалистической экспертизы, а также оптимальными методами их использования. Когда возникает необходимость в выполнении особенно сложных следственных действий, таких как восстановление файлов, которые были удалены, повреждены или закодированы и зашифрованы с

использованием сложных шифров, допускается привлечение внешних экспертов, которые впоследствии могут быть вызваны в суд в качестве свидетелей-экспертов обвинения[124].

216. Любые исследования рекомендуется проводить на дубликате первичных доказательств, для того чтобы сохранить в неприкосновенности подлинные исходные данные[125]. Дубликат цифровых данных может быть создан с использованием специальных инструментов криминалистической экспертизы, таких как утилита EnCase компании Guidance Software, программный продукт Forensic Tool Kit или их бесплатные альтернативы. По мере возможности, для создания дубликатов следует использовать по крайней мере два различных инструмента криминалистической экспертизы на тот случай, если с помощью одного не удастся адекватно собрать все данные[126].

217. С помощью утилиты EnCase копия данных, содержащихся на исследуемом устройстве, создается путем анализа всех секторов жесткого диска, в том числе нераспределенных, чтобы обеспечить захват любых скрытых или удаленных файлов. Данный программный продукт также может быть использован, в частности, для анализа структуры файловой системы цифровых носителей, систематизации анализируемых файлов и создания графического представления или других форм отчетов касательно определенных характеристик этих файлов. EnCase также позволяет создавать и присваивать цифровым уликам уникальные идентификаторы, известные как "значение хеш-функции"[127].

218. В целях подтверждения подлинности цифровых улик в связи с судебным разбирательством (см. раздел D главы IV, ниже) значение хеш-функции, присваиваемое цифровым файлам или их частям, устанавливается на основе применения математических алгоритмов к параметрам соответствующего набора данных. Любое изменение набора данных привело бы к генерации различных значений хеш-функции. Значения хеш-функции вычисляются в отношении: *a)* оригинала жесткого диска до создания его дубликата; *b)* дубликата или дубликатов диска до проведения криминалистической экспертизы и *c)* дубликата или дубликатов диска после проведения экспертизы. Совпадение значений хеш-функции подтверждает вывод, что цифровые данные не были фальсифицированы и что дубликат, подвергшийся криминалистической экспертизе, для целей судопроизводства может рассматриваться как носитель подлинных исходных данных. К числу обычно используемых алгоритмов хеширования относятся MD5 и SHA[128].

D. Подтверждение подлинности цифровых улик

219. Для эффективного осуществления судебного преследования по подозрению в использовании Интернета в террористических целях необходимо подкрепить его собранными надлежащим образом и хорошо документированными доказательствами (см. раздел G.2 главы IV). Это требуется для установления целостности цифровых улик в целях как признания их допустимости в суде, так и придания им большей убедительности. Целостность цифровых улик может быть установлена путем сочетания традиционных и специальных методов ведения следствия. К числу ключевых вопросов относятся режим охраны как физического устройства, использовавшегося для хранения или передачи электронных данных, так и самих данных,

[124] Письменный материал, представленный экспертом из Израиля.

[125] United States, Department of Justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (2004), p. 1. См. по адресу: www.ncjrs.gov/pdffiles1/nij/199408.pdf.

[126] EC-Council Press, *Computer Forensics: Investigating Data and Image Files* (Clifton Park, New York, Course Technology Cengage Learning, 2010), p. 2-4.

[127] Письменный материал, представленный экспертом из Группы специального назначения Корпуса карабинеров Италии.

[128] Barbara J. Rothstein, Ronald J. Hedges and Elizabeth C. Wiggins, Managing discovery of electronic information: a pocket guide for judges (Federal Judicial Center, 2007). См. по адресу: www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf.

а также процедуры, примененные для получения этих данных, и любые отклонения от общепринятых методов. Что касается традиционных методов расследования, то сотрудники правоохранительных органов вправе наводить справки, чтобы установить, по мере возможности, кто мог работать с этими уликами или иметь доступ к ним, до того как на них был наложен арест, и когда, как и откуда эти улики были получены.

220. От прокурора также могут потребоваться доказательства того, в частности, что полученная информация достоверно и точно отображает данные, первоначально содержавшиеся на соответствующем носителе, и что он может продемонстрировать связь с ними обвиняемого. Вычисленные в отношении цифровых улик значения хеш-функции служат убедительным подтверждением того, что такие улики остаются нескомпрометированными. Для установления аутентичности, кроме того, можно представлять дополнительные подкрепляющие доказательства и свидетельские показания. Иллюстрацией этой практики может служить дело Адама Басби, который был осужден в 2010 году в Ирландии за отправку по электронной почте в аэропорт Хитроу в Лондоне сообщения об угрозе применения бомбы. Во время суда над Басби, в дополнение к доказательствам того, что сообщение электронной почты было отправлено с определенного компьютера, к которому обвиняемый имел доступ, были также представлены распечатка журнала регистрации пользования компьютером и телевизионная запись со скрытыми титрами, чтобы установить время, когда было передано сообщение электронной почты, и доказать тот факт, что в это время за компьютером работал именно обвиняемый.

E. Оперативные подразделения по борьбе с киберпреступностью

1. Национальные или региональные подразделения по борьбе с киберпреступностью

221. Рост зависимости от компьютерных технологий ведет к резкому увеличению потребности в специализированных подразделениях по борьбе с киберпреступностью, призванных откликаться на запросы о поиске улик в виде компьютерных данных с помощью криминалистических средств, причем не только по делам, связанным с использованием Интернета террористами. Примеры случаев использования Интернета в преступных целях особенно распространены в сфере организованной преступности, такой как незаконный оборот наркотиков, торговля людьми и деятельность международных групп педофилов, однако в последние годы диапазон дел, в которых в той или иной форме фигурируют доказательства в виде компьютерных или электронных данных, становится все шире. Создание национальных подразделений по борьбе с киберпреступностью, обладающих специальными навыками, необходимыми для расследования киберпреступлений, могло бы значительно расширить оперативные возможности государств по удовлетворению таких потребностей. В зависимости от географических особенностей и потребностей в ресурсах в поддержку таким общенациональным подразделениям могут также создаваться менее крупные региональные подразделения для принятия ответных мер на местах. Кроме того, если командование региональными подразделениями будет осуществляться местными органами регионального управления, это может оказаться более эффективным и рентабельным.

222. Обязанности национальных или региональных подразделений по борьбе с киберпреступность могут включать:

a) сбор разведывательных данных из открытых источников с помощью специальных методов наблюдения в режиме онлайн за сайтами социальных сетей, дискуссионными группами, веб-сайтами и электронными досками объявлений в Интернете в целях выявления деятельности террористических групп (а также многих других преступных элементов). В отношении террористических групп эту функцию можно было

бы отнести к компетенции подразделений по борьбе с терроризмом, сотрудники которых имеют достаточную подготовку и опыт, чтобы решать соответствующие задачи, однако считается, что для выполнения этой роли важнейшее значение имеет специальная подготовка в области борьбы с киберпреступностью. Выполнение функции по сбору разведывательных данных также требует их оценки и анализа в целях содействия выработке стратегии по противостоянию угрозе, связанной с использованием Интернета террористами. Однако координации действий и переводу данных разведки в эффективные оперативные планы может препятствовать несовместимость обязанностей или задач, возлагаемых на различные национальные спецслужбы;

b) проведение в рамках борьбы с киберпреступностью специальных расследований по делам на национальном и международном уровнях, касающимся преступлений, которые связаны с использованием технологий, например таких преступлений, как мошенничество или кража данных в Интернете, и по другим делам, в отношении которых возникают сложные технологические, правовые и процедурные вопросы и которые, по оценке руководства подразделения по борьбе с киберпреступностью, требуют задействования специальных средств ведения расследования, имеющихся в распоряжении данного подразделения;

c) выполнение роли связующего звена на межотраслевом и международном уровнях в целях установления партнерских связей с основными заинтересованными сторонами в области борьбы с киберпреступностью, такими как сектор финансовых услуг, сектор телекоммуникационных услуг, компьютерная отрасль, соответствующие государственные ведомства, научные учреждения и межправительственные или региональные организации;

d) обеспечение функционирования группы оценки, призванной производить оценку связанных с киберпреступностью дел на национальном и международном уровнях в целях установления приоритетов при проведении расследований национальными или региональными подразделениями по борьбе с киберпреступностью. На такую группу можно также возложить функции по ведению статистики о распространенности случаев совершения киберпреступлений;

e) обеспечение подготовки кадров и проведение научных исследований и разработок, поскольку в связи со сложным и меняющимся характером киберпреступности национальные и региональные подразделения должны опираться на научную поддержку специализированных научных учреждений, что гарантирует сохранение должного уровня квалификации их персонала и предоставление им всех технических средств, обеспечение профессиональной подготовки и образования, необходимых для криминалистического исследования носителей компьютерных данных и расследования киберпреступлений.

2. Группы по сортировке компьютерной техники в судебных целях

223. В помощь национальным и региональным подразделениям по борьбе с киберпреступностью могут создаваться группы по сортировке компьютерной техники в судебных целях. Сотрудники таких подразделений должны быть обучены методам криминалистической оценки элементов компьютеров с использованием специально разработанных программных средств на месте проведения обыска. Члены группы по сортировке компьютерной техники могут провести первичное обследование на месте, чтобы либо исключить компьютер или другие периферийные компьютерные устройства из следствия как не имеющие доказательной ценности, либо произвести выемку связанных с компьютером улик с соблюдением надлежащих криминалистических процедур, а также оказать содействие местным следственным группам в проведении допроса подозреваемых в отношении обнаруженных улик, которые имеют отношение к компьютеру. Если потребуется, изъятые группами по сортировке элементы

компьютерной техники также могут, в зависимости от обстоятельств, быть переданы в соответствующее региональное или национальное подразделение по борьбе с киберпреступностью в целях проведения полноценной криминалистической экспертизы.

224. Исследователи из Университетского колледжа Дублина в настоящее время занимаются разработкой ряда программных средств, предназначенных для криминалистических исследований, которые будут содействовать проведению предварительного анализа и будут предоставляться сотрудникам правоохранительных органов на безвозмездной основе. Разработка этих инструментов ведется в рамках поиска более широкого стратегического решения, над которым работают Центр по вопросам кибербезопасности и расследования киберпреступлений при Университетском колледже Дублина, а также Группа по расследованию компьютерных преступлений Национальной полицейской службы Ирландии (An Garda Siochâna) и которое имеет целью оказание помощи подразделениям по борьбе с киберпреступностью, не получающим достаточного ресурсного обеспечения и испытывающим нехватку бюджетных средств и персонала для решения стоящих перед ними задач. Целью этой инициативы станет создание криминалистической лаборатории, полностью работающей на основе "открытых источников информации". Участвующие в ней следователи пройдут обучение по вопросам, касающимся создания хранилищ улик в виде компьютерных данных и работы с оборудованием для их обработки, а также получат подготовку по использованию бесплатного криминалистического программного обеспечения.

F. Сбор информации

225. Сбор разведывательных данных является одним из ключевых компонентов деятельности по борьбе с терроризмом, а получаемая по таким каналам информация нередко становится основанием для расследований, которые ведут к уголовному преследованию подозреваемых, или используется в качестве средств доказывания в суде в пределах, разрешенных национальным законодательством и процессуальными нормами. Однако, поскольку сбор разведывательной информации может осуществляться в различных целях, а собирать или использовать эту информацию могут различные учреждения, может возникнуть необходимость в тщательном согласовании противоречащих друг другу интересов. Например, участвующие в сборе разведывательной информации правоохранительные органы или спецслужбы могут уделять особое внимание защите конфиденциальности источника информации, в то время как должностным лицам суда приходится учитывать, в частности, право обвиняемого на справедливое судебное разбирательство и равный доступ к представляемым против него или нее доказательствам. Должное внимание надлежит уделять обеспечению адекватных сдержек и противовесов в отношении соблюдения основных прав человека, закрепленных в соответствующих международных конвенциях[129].

226. В ряде государств-членов информация из анонимных источников не допускается в качестве доказательства в суде; однако разведывательные сведения, подтвержденные авторитетными источниками или дополнительными доказательствами, могут быть приняты к рассмотрению. Например, в Ирландии собранные в отношении террористов разведывательные данные могут считаться достаточно достоверным доказательством того, что то или иное конкретное лицо является членом незаконной организации, если соответствующие показания дает под присягой сотрудник полиции в ранге не ниже старшего суперинтендента. Верховный суд Ирландии поддержал использование такой разведывательной информации в качестве доказательства при наличии подкрепляющих доказательств, когда получить прямые

[129] См., например, Всеобщую декларацию прав человека, статью 10; Международный пакт о гражданских и политических правах, статью 14; и Европейскую конвенцию о защите прав человека и основных свобод, статью 6.

доказательства невозможно из-за страха перед репрессалиями, а также с учетом высокого ранга сотрудника, дававшего показания[130].

227. Некоторые эксперты также обращают внимание на существование противоречия между необходимостью содействовать получению сведений о потенциальной террористической деятельности, осуществляемой через Интернет, и необходимостью задержания и судебного преследования виновных в ведении такой деятельности. Например, после того как будет установлено, что на веб-сайте ведется деятельность, потенциально связанная с терроризмом, агентствам национальной безопасности, видимо, следует обдумать долгосрочные и краткосрочные последствия ответных оперативных мер, которые им надлежит принять. Такие ответные меры могут включать пассивный мониторинг деятельности веб-сайта в разведывательных целях, скрытное установление контактов с другими пользователями для получения дополнительных сведений в контртеррористических целях или закрытие соответствующего веб-сайта. Выбор предпочтительного метода ведения борьбы с терроризмом может определяться рядом целей и стратегиями различных национальных и зарубежных агентств[131].

228. Практические соображения, учитываемые при определении важности разведывательной информации в сравнении с уровнем угрозы, которую представляет тот или иной интернет-ресурс, были освещены в недавнем докладе Исследовательской службы конгресса Соединенных Штатов.

> Например, как сообщают, [Центральным разведывательным управлением] и правительством Саудовской Аравии был разработан в качестве "приманки" джихадистский веб-сайт в целях привлечения террористов и установления контроля за их деятельностью. Собранная на сайте информация была использована аналитиками разведывательных служб для отслеживания оперативных планов джихадистов, в результате чего их удалось арестовать до того, как планируемые нападения могли быть осуществлены. Однако, судя по сообщениям, данный сайт также использовался для передачи оперативных планов джихадистам, направлявшимся в Ирак в целях проведения нападений на военнослужащих США. В ходе обсуждений между представителями [Агентства национальной безопасности, Центрального разведывательного управления, Министерства обороны, Управления Директора национальной разведки и Совета национальной безопасности] было установлено, что угроза военнослужащим, участвующим в военных действиях, превышала разведывательную ценность информации, получаемой за счет мониторинга веб-сайта, и в конечном счете он был демонтирован группой специалистов по компьютерным сетям из [Объединенной оперативной группы Сети глобальных операций][132].

Вышеприведенный пример показывает, что межведомственная координация является важным фактором успешного реагирования на выявляемые угрозы.

229. Другие государства-члены, такие как Соединенное Королевство, отмечают, что они уделяют значительное внимание установлению рабочих отношений и подписанию меморандумов о взаимопонимании между органами прокуратуры и правоохранительными или разведывательными органами, что приносит положительные результаты. Аналогичным образом, в Колумбии Объединенный центр разведки и расследований (Centro Integrado de Inteligencia e Investigaciôn, или CI3) является национальным агентством, которое осуществляет координацию расследований по подозрению в террористической деятельности на основе стратегии, базирующейся на шести основных принципах. В рамках этого подхода общее командование

[130] *People (DPP) v. Kelly*, [2006] 3 I.R. 115.

[131] Catherine Theohary and John Rollins, Congressional Research Service (United States), "Terrorist use of the Internet: information operations in cyberspace" (8 March 2011), p. 8.

[132] Ibid, p. 13.

и управление на разных этапах расследования, включая сбор, засвидетельствование и анализ доказательств, и на судебной стадии, в ходе которой полиция собирает сведения о лицах и местах, связанных с совершением тех или иных преступлений, берут на себя высокопоставленные служащие национальной полиции[133].

230. Эксперт из Франции обрисовал принятый в его стране подход к координации принимаемых на межучрежденческом уровне мер в ответ на выявленную террористическую деятельность.

- Этап 1. Службы наблюдения и разведки выявляют угрозы путем мониторинга деятельности в Интернете.
- Этап 2. Службы наблюдения уведомляют службы государственного обвинения о выявленной угрозе. После этого судья или прокурор может дать правоохранительным органам разрешение на установление наблюдения за деятельностью выявленного подозреваемого в Интернете. Начиная с 2011 года законодательство позволяет главному судье давать правоохранителям разрешения на ведение записи компьютерных данных поднадзорного. Кроме того, личные данные (например, имя, номер телефона, номер кредитной карты) разрешается запрашивать у соответствующих провайдеров услуг Интернет.
- Этап 3. Расследование проводится на основании доказательств, собранных из источников, указанных в рамках этапов 1 и 2.

G. Подготовка персонала

231. Сотрудники правоохранительных органов, участвующие в расследованиях по использованию Интернета в террористических целях, должны пройти специальную подготовку по техническим аспектам возможных способов использования Интернета террористами и другими преступниками в целях содействия достижению противозаконных целей, а также изучить возможные методы эффективного использования Интернета правоохранительными органами в качестве ресурса для отслеживания деятельности террористических групп. Такое обучение может осуществляться в рамках инициатив государственного или частного секторов или посредством сочетания тех и других.

232. Курсы по криминалистической экспертизе в области информационных технологий и расследованию киберпреступлений могут быть организованы на региональном или международном уровне такими организациями, как Европол и Интерпол. Кроме того, в ряде стран, либо самостоятельно, либо в сотрудничестве с академическими институтами, разработаны собственные учебные программы по вопросам борьбы с киберпреступностью для сотрудников правоохранительных органов. Обучение также может вестись в рамках специальных учебных курсов, семинаров, конференций и практических занятий, организуемых с помощью заинтересованных сторон в государственном секторе и соответствующих отраслях промышленности.

233. Специализированная подготовка может также осуществляться в академических институтах, таких как Университетский колледж Дублина в Ирландии, при котором в 2006 году был создан Центр по вопросам кибербезопасности и расследования киберпреступлений. В число предлагаемых этим университетом программ входит предназначенная только для сотрудников правоохранительных органов программа магистратуры в области применения компьютеров в целях криминалистической экспертизы и расследования киберпреступлений.

[133] Управление Организации Объединенных Наций по наркотикам и преступности, Обзор дел о терроризме, пункт 191.

Дополнительно существуют также курсы по подготовке специалистов оперативного реагирования к выполнению ими своих оперативных функций в делах, связанных с киберпреступностью.

234. Сеть центров повышения квалификации для профессиональной подготовки, научных исследований и образования в области борьбы с киберпреступностью (2CENTRE) представляет собой финансируемый Европейской комиссией проект, реализация которого началась в 2010 году в целях создания сети центров повышения квалификации для профессиональной подготовки, научных исследований и образования в области борьбы с киберпреступностью в Европе. В настоящее время такие центры создаются в Бельгии, Ирландии, Франции и Эстонии. Каждый из национальных центров основан на партнерстве между представителями правоохранительных органов, промышленных и научных кругов, которые сотрудничают друг с другом в целях разработки соответствующих учебных программ и квалификационных требований, а также инструментов для использования в борьбе с киберпреступностью. Руководителем и координатором проекта является Центр по вопросам кибербезопасности и расследования киберпреступлений при Университетском колледже Дублина[134].

235. Курс обучения по вопросам борьбы с терроризмом можно также пройти в Интернете в рамках начала работы в 2011 году Контртеррористической учебной платформы ЮНОДК[135]. Эта платформа представляет собой интерактивный механизм, специально предназначенный для обучения специалистов-практиков системы уголовного правосудия методам борьбы с терроризмом в процессе их объединения в единое виртуальное сообщество, где они могут делиться своим опытом и мнениями в отношении борьбы с терроризмом. Кроме того, что она дает специалистам-практикам, которые ранее уже участвовали в организуемых ЮНОДК курсах профессиональной подготовки, возможность связываться друг с другом и формировать сетевые связи со своими коллегами, данная платформа позволяет им быть в курсе эволюции правовой базы в данной области, узнавать о предстоящих возможностях обучения и участвовать в непрерывном учебном процессе.

[134] См. www.2centre.eu.

[135] См. www.unodc.org/unodc/en/terrorism/unodc-counter-terrorism-learning-platform.html (на английском, испанском и французском языках).

V. Международное сотрудничество

A. Введение

236. Скорость, глобальный охват и относительная анонимность, с которой террористы могут использовать Интернет для продвижения своего дела или содействия совершению террористических актов, в сочетании со сложностями, связанными с обнаружением, обеспечением сохранности, изъятием и представлением данных, связанных с Интернетом, делают своевременное и эффективное международное сотрудничество между правоохранительными и разведывательными органами все более важным фактором в успешном расследовании многих дел, касающихся терроризма, и судебном преследовании в связи с ними.

B. Документы и договоренности по вопросам международного сотрудничества

1. Универсальные документы по борьбе с терроризмом

237. В универсальных документах по борьбе с терроризмом, к числу которых относятся международные конвенции и протоколы, а также соответствующие резолюции Совета Безопасности, содержатся комплексные механизмы международного сотрудничества в осуществлении уголовного преследования по делам, связанным с терроризмом. Этими документами предусматриваются выдача преступников, оказание взаимной правовой помощи, передача уголовных дел и осужденных, взаимное исполнение судебных решений, замораживание и конфискация активов и обмен информацией между правоохранительными органами.

238. Ключевыми элементами документов по борьбе с терроризмом, касающихся международного сотрудничества, являются:

- обязательство привлекать к судебной ответственности виновных в совершении террористических актов;
- обязательство выдать или предать суду (принцип aut dedere aut judicare);
- обязательство установить судебную юрисдикцию в заданных обстоятельствах;
- обязательство не допускать использования исключения для политических преступлений в качестве основания для отказа в просьбе о сотрудничестве;
- уважение принципа верховенства права и прав человека;
- соблюдение принципа "двойной уголовной ответственности";
- соблюдение нормы о неизменности квалификации условий;
- соблюдение нормы ne bis in idem: недопустимость повторного преследования за совершение одного и того же преступления[136].

239. Общие принципы, применимые к выдаче и оказанию взаимной правовой помощи по делам, связанным с терроризмом и транснациональной организованной преступностью, являются составной частью всеобъемлющих механизмов, описанных в универсальных доку-

[136] Управление Организации Объединенных Наций по наркотикам и преступности, Пособие по международному сотрудничеству в области уголовного правосудия в связи с терроризмом (2009 год), раздел 1.C.

ментах по борьбе с терроризмом и других документах, касающихся борьбы с транснациональной организованной преступностью (например, Конвенции Организации Объединенных Наций против транснациональной организованной преступности)[137]. В настоящей публикации не ставится цель вновь подробно подтверждать или анализировать, как эти принципы должны претворяться в жизнь государствами на национальном уровне. Скорее, акцент в ней делается на выявлении, в рамках установленного благодаря этим документам широкого международного сотрудничества и на основании общепризнанных принципов и механизмов, вопросов, конкретно относящихся к делам о терроризме, связанным с использованием Интернета, для того чтобы служить руководством для лиц, определяющих политику, и специалистов-практиков в отношении подходов и стратегий, отражающих современную передовую практику.

a) Отсутствие универсального документа по проблемам киберпреступности

240. Хотя механизмы международного сотрудничества, предусмотренные в универсальных документах по борьбе с терроризмом, когда они будут реализованы в полном объеме, по-видимому, смогут служить правовой основой для сотрудничества во многих случаях, касающихся связанных с использованием Интернета деяний со стороны лиц, причастных к совершению противоправных деяний, указанных в этих документах, ни один из них не касается именно действий, связанных с Интернетом, как таковых. В отсутствие документа по борьбе с терроризмом, конкретно касающегося имеющих отношение к терроризму проблем Интернета, компетентные органы при проведении расследований и судебного преследования по таким делам будут по-прежнему опираться на существующие международные или региональные соглашения либо договоренности, заключенные в целях содействия международному сотрудничеству при расследовании и осуществлении судебного преследования за преступления, связанные с терроризмом или транснациональной организованной преступностью в целом.

241. Очевидно, что отсутствие универсального документа, конкретно посвященного информационным технологиям, в некоторой степени затрудняет международное сотрудничество в вопросах расследования и уголовного преследования по делам о терроризме, связанным с использованием Интернета террористами. Однако в настоящей публикации не стоит цель оценивать относительные достоинства аргументации за или против целесообразности выработки всеобъемлющего универсального документа по вопросам, в частности, международного сотрудничества в уголовных делах (в том числе о терроризме), связанных с применением компьютерной техники. Основное внимание в ней скорее уделяется выявлению в рамках нынешней международной структуры областей, которые становятся препятствиями на пути такого сотрудничества, а также тому, каким образом национальные органы власти могли бы использовать существующие и доступные документы и договоренности для содействия или укрепления международного сотрудничества по делам о терроризме, связанным с какими-либо аспектами использования Интернета.

b) Другие документы: Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция Совета Европы о киберпреступности

242. Конвенция Организации Объединенных Наций против транснациональной организованной преступности является основным международным документом, регулирующим международное сотрудничество между государствами по серьезным делам, связанным с транснациональной организованной преступностью. Вопросам международного сотрудничества посвящены статьи 16 (Выдача), 18 (Взаимная правовая помощь), 19 (Совместные

[137] United Nations, *Treaty Series*, vol. 2225, No. 39574.

расследования) и 27 (Сотрудничество между правоохранительными органами) Конвенции против организованной преступности. Хотя противоправное поведение, о котором идет речь в Конвенции против организованной преступности, относится к сфере транснациональной организованной преступности, а не терроризма, основополагающие принципы и механизмы данной Конвенции, касающиеся международного сотрудничества, весьма сходны с принципами и механизмами, содержащимися в универсальных документах по борьбе с терроризмом. Таким образом, государства-участники, выполнившие свои международные обязательства в отношении сотрудничества в рамках этих документов, должны располагать совместимыми в общих чертах структурами и механизмами.

243. В дополнение к Конвенции Совета Европы о киберпреступности правовой основой для международного сотрудничества по делам о терроризме, связанным с некоторыми элементами использования Интернета, могут служить Конвенция Совета Европы о предупреждении терроризма, Европейская конвенция о выдаче[138] и три дополнительных протокола к ней[139], Европейская конвенция о взаимной помощи по уголовным делам[140] и два дополнительных протокола к ней[141], а также Акт Совета Европейского союза № 2000/C 197/01 [от 29 мая 2000 года] об утверждении, согласно статье 34 Договора о Европейском союзе, Конвенции о взаимной помощи в уголовных делах между государствами – членами Европейского союза.

244. В Конвенции Совета Европы о киберпреступности содержатся положения, направленные на поощрение международного сотрудничества в рамках механизмов сотрудничества органов полиции и судебных органов, а также положения о принятии временных мер в экстренных случаях, например, о неофициальном предоставлении внеплановой информации по запросам (статья 26) и о создании пунктов связи, доступных 24 часа в сутки семь дней в неделю (статья 35). Такие запросы могут сопровождаться требованиями о неразглашении и являются правовым механизмом, позволяющим использовать неофициальные средства связи и обмена информацией между сторонами Конвенции, даже если в их национальном законодательстве подобные положения отсутствуют.

245. Следует отметить, что Конвенция Совета Европы о киберпреступности открыта не только для членов Совета Европы или государств, не являющихся его членами, которые принимали участие в ее разработке, но к ней могут также присоединиться и другие страны, не являющиеся его членами, в последнем случае с единодушного согласия договаривающихся государств, правомочных заседать в Комитете министров.

2. Другие региональные или многосторонние договоренности

246. В дополнение к упомянутым выше международным и региональным документам государства могут принять решение о заключении двусторонних или многосторонних соглашений или договоренностей, содержащих конкретные положения о сотрудничестве в проведении мероприятий в области информационных технологий, связанных с борьбой против терроризма и транснациональной преступности. Вопросы выдачи и взаимной правовой помощи, как правило, регулируются либо договорами, либо согласованными между блоками стран нормами "мягкого права". Вместе с тем важная роль в содействии обмену информацией и обеспечению сотрудничества в рамках таких взаимосогласованных договоренностей также принадлежит региональным и субрегиональным организациям.

[138] Council of Europe, *European Treaty Series*, No. 24.

[139] Ibid., Nos. 86, 98 and 209.

[140] Ibid., No. 30.

[141] Ibid., Nos. 99 and 182.

a) Европейский ордер на арест: шенгенская система

247. Европейский ордер на арест в рамках шенгенской системы является инструментом сотрудничества, применимым во всех государствах – членах Европейского союза; он оказался чрезвычайно полезным для укрепления правового сотрудничества в расследовании и преследовании по уголовным делам, в том числе связанным с терроризмом в Европе. Будучи выдан, такой ордер обязывает органы власти других государств-членов, на основе взаимности, арестовать и передать подозреваемого преступника или осужденного государству, выдавшему ордер, для того чтобы соответствующее лицо могло быть предано суду или для отбытия им срока наказания. В данном контексте следует отметить, что европейский ордер на арест предполагает, в частности, выдачу собственных граждан государств-членов, хотя прежде такая концепция была чуждой для правовых (зачастую конституционных) норм многих государств, придерживающихся так называемой континентальной европейской системы.

b) Европейский ордер на сбор доказательств

248. С момента вступления в силу в 2009 году европейский ордер на сбор доказательств, подобно европейскому ордеру на арест в отношении производства арестов, привел к созданию упрощенной процедуры сбора и передачи средств доказывания, включая предметы, документы и данные, между государствами-членами в целях их использования в уголовном судопроизводстве. По условиям европейского ордера на сбор доказательств, собранные улики могут включать пользовательские данные, связанные с деятельностью в Интернете[142].

249. На основе этих рамочных решений и других международных документов европейские государства, выступая в качестве единого блока, утвердили продвинутый, в широком смысле коллективный подход к трансграничному сбору и пересылке доказательств, а также к выдаче/передаче правонарушителей в целях их уголовного преследования. Прочие правительства могли бы рассмотреть на политическом и оперативном уровнях вопрос о желательности принятия и адаптации коллективного подхода в рамках региона или субрегиона к согласованию своих усилий по налаживанию сотрудничества при проведении трансграничных расследований и уголовного преследования за преступления, связанные с терроризмом.

c) Программы Содружества в отношении выдачи и взаимной правовой помощи

250. По аналогии с действующим в рамках шенгенской системы европейским ордером на арест, Программа передачи осужденных правонарушителей в рамках Содружества (Лондонская программа) предлагает упрощенный механизм выдачи между странами – членами Содружества, предусматривающий возможность предварительного ареста правонарушителей на основании ордера на арест, выданного другими странами-членами, без необходимости оценки достаточности доказательственных материалов для обвинения подозреваемого. В соответствии с этой Программой предполагается, что правонарушения могут служить основанием для выдачи, если они считаются преступлениями в обеих странах и влекут за собой наказание в виде лишения свободы сроком на два года или более.

251. Аналогичным образом, Программа Содружества по оказанию взаимной правовой помощи (Программа Хараре) имеет целью повышение уровня и объемов помощи по уголовным делам, оказываемой друг другу странами Содружества, путем упрощения процессов идентификации и установления местонахождения разыскиваемых лиц, официального вручения документов, допроса свидетелей, проведения обысков и изъятия улик, обеспечения явки свидетелей, временной передачи лиц, содержащихся под стражей, в целях дачи показаний, представления судебных или официальных материалов, отслеживания, ареста и конфискации

[142] Voislav Stojanovski, "The European evidence warrant", in *Dny práva—2009—Days of Law: the Conference Proceedings*, 1st. ed., David Sehnálek and others, eds. (Brno, Czech Republic, Masaryk University, 2009).

доходов от преступления или средств совершения преступления, а также сохранения компьютерных данных.

252. Хотя программы Содружества как таковые не считаются договорами, они являются примерами не имеющих обязательной силы договоренностей, или "мягкого права", в рамках которых ряд стран соглашаются внести в свое внутреннее законодательство совместимые законоположения, отвечающие согласованным принципам, в целях упрощения выдачи и оказания взаимной правовой помощи по уголовным делам, в том числе в расследованиях и судопроизводстве по делам, связанным с терроризмом.

d) Совет Европы

253. Наряду с разработкой документов, направленных на развитие международного сотрудничества по связанным с использованием интернет-технологий уголовным делам, в том числе о терроризме, Совет Европы также создал (согласно статье 35 Конвенции Совета Европы о киберпреступности) Сеть 24/7 Совета Европы, объединяющую контактные центры, работающие 24 часа в сутки семь дней в неделю, цель которой состоит в содействии международному сотрудничеству по делам, касающимся киберпреступности. Региональные проекты Совета Европы и Европейского союза, в том числе Cybercrime@IPA и Cybercrime@EAP, финансируют участие контактных центров Сети 24/7 в учебных мероприятиях, в ходе которых им предоставляется возможность связываться друг с другом, а также подключаться к сети членов Группы восьми (G-8).

254. С 2006 года Совет Европы в рамках своего Глобального проекта по борьбе с киберпреступностью оказывает содействие странам во всем мире в совершенствовании законодательства, профессиональной подготовке судей, обвинителей и следователей правоохранительных органов по вопросам, связанным с киберпреступностью и сбором доказательств в электронной форме, а также в налаживании взаимодействия между правоохранительными органами и провайдерами услуг Интернет и организации международного сотрудничества[143]. С 2010 года одной из сфер повышенного внимания стали связанные с преступностью денежные потоки и финансовые расследования в Интернете, в том числе в отношении финансирования террористов через Интернет[144].

e) План действий Европейского союза: центр по борьбе с киберпреступностью

255. 26 апреля 2010 года, признавая неотъемлемую составляющую роль информационных и коммуникационных технологий в современном обществе, а также рост числа, масштабов, изощренности и потенциальных последствий угроз для ряда юрисдикций, в связи с чем возрастает необходимость укрепления сотрудничества между государствами-членами и частным сектором, Совет Европейского союза одобрил выводы в отношении плана действий по борьбе с киберпреступностью, который должен быть включен в Стокгольмскую программу на 2010–2014 годы и связанную с ней будущую Стратегию внутренней безопасности.

256. В рамках этого плана члены Совета согласились, в частности, поручить Европейской комиссии во взаимодействии с Европолом проанализировать вопрос о полезности и целесообразности создания Европейского центра по борьбе с киберпреступностью в целях расширения базы знаний, потенциала и сотрудничества в области борьбы с киберпреступностью и представить соответствующий отчет. По завершении этой работы было выработано предложение, согласно которому в Европоле должна быть создана новая служба, которая будет получать и обрабатывать аналитические рабочие файлы, касающиеся серьезной организованной преступности и терроризма.

---

[143] См. www.coe.int/lportal/web/coe-portal/what-we-do/rule-of-law/terrorism.

[144] Council of Europe, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, *Criminal Money Flows on the Internet: Methods, Trends and Multi-Stakeholder Counteraction* (2012).

3. Роль других региональных организаций и соглашений о сотрудничестве

257. Как отмечалось выше, соглашения об официальном сотрудничестве на региональном и субрегиональном уровнях между правоохранительными и разведывательными службами являются неотъемлемой частью усилий международного сообщества по укреплению и координации мер, направленных на борьбу с терроризмом и транснациональной организованной преступностью. Хотя сотрудничество в рамках этих договоренностей, как правило, не основывается на базе юридически обязательных договоров или иных документов, оно тем не менее может вести к созданию в высшей степени эффективных механизмов взаимодействия между участвующими странами-членами.

258. На международном уровне существует немало примеров таких договоренностей, однако три из них, действующие в Европе, Африке и Тихоокеанском регионе, показывают, каким образом группы стран с совпадающими интересами и целями в области обеспечения правопорядка и безопасности могут успешно действовать совместно в целях развития и согласования тесного сотрудничества в проведении уголовных расследований.

259. Франко-германский Центр сотрудничества полицейских и таможенных служб, известный также как Оффенбургский центр, был создан в 1998 году в целях, в частности, содействия координации межведомственных операций (например, операций по розыску и наблюдению, а также обмену собранной информацией), проводимых по обе стороны общей границы между этими странами. Центр укомплектован сотрудниками полицейских, таможенных и пограничных ведомств федерального и регионального уровня и ежегодно обрабатывает многие тысячи запросов, выступая в качестве платформы для посредничества в целях выработки прагматических решений в ответ на возникающие между учреждениями-партнерами проблемы и для развития доверия и сотрудничества между соответствующими ведомствами.

260. В Африке члены Южноафриканской региональной организации по сотрудничеству начальников полиции и Восточноафриканской организации сотрудничества начальников полиции договорились о том, в каких конкретных областях будет развиваться сотрудничество органов полиции, включая регулярный обмен связанной с преступностью информацией; планирование, координацию и проведение совместных операций, в том числе тайных; осуществление пограничного контроля и мер по предупреждению преступности в приграничных районах, а также последующих операций; осуществление контролируемых поставок запрещенных веществ или любых других предметов; а также оказание, по необходимости, технической и экспертной помощи[145].

261. В Тихоокеанском регионе центром деятельности по сбору, координации, анализу и обмену данными полицейской разведки, собираемыми в рамках сети национальных групп по борьбе с транснациональной преступностью, которые действуют в странах-членах по всему региону, является Тихоокеанский центр координации борьбы с транснациональной преступностью. Этот Центр, в котором работают прикомандированные сотрудники правоохранительных органов и пограничных ведомств из различных тихоокеанских островных стран, предоставляет странам-членам точку доступа к Интерполу и другим правоохранительным учреждениям по всему миру через международную сеть поддерживающей данную инициативу Федеральной полиции Австралии.

262. Аналогичным образом, коллективные договоренности, предусматривающие обмен разведывательной информацией и ее совместное использование, могут также заключать страны, не обязательно близкие географически, но имеющие общие интересы в тех или иных тематических областях, связанных с обеспечением правопорядка и безопасности.

[145] Charles Goredema, "Inter-State cooperation", в *African Commitments to Combating Organised Crime and Terrorism: A review of eight NEPAD countries* (African Human Security Initiative, 2004). См. по адресу: www.iss.co.za/pubs/Other/ahsi/Goredema_Botha/pt1chap5.pdf.

a) Эгмонтская группа подразделений финансовой разведки

263. Одним из примеров таких договоренностей является Эгмонтская группа подразделений финансовой разведки, действующая в сфере расследований, касающихся финансирования терроризма. Расследования по подозрению в финансировании терроризма неизменно сопряжены со сбором, обменом и анализом финансовой или банковской документации, находящейся в одной или нескольких юрисдикциях. В этих случаях наличие у подразделений финансовой разведки возможности работать в сотрудничестве и обмениваться секретной финансовой информацией может иметь решающее значение для успешного расследования и судебного преследования. Эгмонтская группа – созданный в 1995 году международный орган – ведет работу по развитию и совершенствованию сотрудничества между подразделениями финансовой разведки в их усилиях по борьбе с отмыванием денег и финансированием терроризма, а также в том числе по содействию расширению и систематизации международного сотрудничества в области взаимного обмена информацией. Эгмонтская группа рекомендует своим членам заключать меморандумы о взаимопонимании, в которых они соглашаются обмениваться секретной финансовой информацией, имеющей отношение к расследованию и уголовному преследованию по делам о финансировании терроризма, отмывании денег и связанной с этим преступной деятельности.

264. В целях обеспечения для национальных подразделений финансовой разведки необходимого потенциала, позволяющего им эффективно сотрудничать по таким делам с иностранными коллегами, органам власти надлежало бы рассмотреть вопрос о целесообразности заключения соответствующих соглашений или договоренностей об обмене информацией с зарубежными партнерами. Полезные указания в отношении видов вопросов, которые, возможно, следовало бы в них охватить, содержатся в предложенном Эгмонтской группой типовом меморандуме о взаимопонимании.

b) Международная организация уголовной полиции

265. Многие международные документы, включая Международную конвенцию о борьбе с финансированием терроризма[146] (пункт 4 статьи 18) и Конвенцию Организации Объединенных Наций против транснациональной организованной преступности (пункт 13 статьи 18), а также различные резолюции Совета Безопасности, в том числе резолюция 1617 (2005), конкретно призывают страны к работе в рамках механизмов Интерпола по сотрудничеству в области обмена информацией.

266. Одной из основных функций Интерпола является содействие международному сотрудничеству между национальными правоохранительными органами и быстрому и безопасному обмену касающейся преступной деятельности информацией и ее анализу. Это осуществляется через посредство его системы I-24/7 (Всемирная система связи полицейских служб), доступ к которой открыт для сотрудников правоохранительных органов всех стран-членов.

267. Используя систему I-24/7, национальные центральные органы получают возможность искать и перепроверять широкий спектр данных, включая информацию о подозреваемых в терроризме и о различных базах данных. Целью этой системы является содействие более эффективному проведению уголовных расследований путем предоставления следователям более широкого круга информации.

268. В дополнение к сети I-24/7 действует программа Интерпола по борьбе с киберпреступностью, направленная на содействие обмену информацией между странами-членами в рамках региональных рабочих групп и конференций, организацию учебных курсов в целях установления и поддержания профессиональных стандартов, координацию международных операций

[146] United Nations, *Treaty Series*, vol. 2178, No. 38349.

и содействие в их проведении, создание глобального списка должностных лиц для контактов по вопросам расследования преступлений в Интернете, оказание помощи странам-членам в случае расследования компьютерных атак или преступлений в Интернете путем предоставления услуг следователей и баз данных, создание стратегических партнерств с другими международными организациями и организациями частного сектора, выявление вновь возникающих угроз и обмен этими сведениями со странами-членами, а также предоставление безопасного веб-портала для доступа к оперативной информации и документам[147].

269. С 2009 года Интерпол работает в тесном сотрудничестве с Университетским колледжем Дублина, обеспечивая подготовку специалистов и осуществление научных обменов в целях содействия повышению квалификации сотрудников правоохранительных органов в области расследования киберпреступлений. В августе 2011 года следователи по делам о преступлениях в Интернете и специалисты по компьютерной криминалистике из 21 страны впервые прошли курс обучения в летней школе по борьбе с киберпреступностью, организованной Интерполом/Университетским колледжем Дублина. Разработанная в Университете двухнедельная программа включала практические занятия на основе имитации судебных дел, которые вели профессионалы из правоохранительных органов, Университетского колледжа Дублина и учреждений частного сектора. Целью данного мероприятия было развитие теоретических и практических знаний и навыков в ряде областей, чтобы помочь следователям более эффективно вести расследование преступлений в Интернете; участники приобрели навыки в таких областях, как создание образа диска, криминалистическое исследование реальных данных, криминалистическое исследование мобильных телефонов, расследование дел, связанных с отмыванием денег, методы производства обысков и изъятий, расследование дел с использованием интернет-телефонии и беспроводных сетей, а также выявление и анализ вредоносных программ[148].

270. Наконец, Отдел Интерпола по преступлениям, связанным с использованием высоких технологий, содействует оперативному сотрудничеству между странами-членами в рамках глобальных и региональных совещаний групп экспертов по киберпреступности и учебных семинаров, а также сотрудничеству между правоохранительными, промышленными и академическими кругами. Он также оказывает помощь странам-членам в случае компьютерных атак и в расследовании киберпреступлений путем предоставления услуг следователей и баз данных.

c) Европейское полицейское управление

271. В значительной степени мандат Европола заключается в повышении эффективности правоохранительных органов государств – членов Европейского союза и укреплении сотрудничества между ними в области предупреждения терроризма и других форм транснациональной организованной преступности и борьбы с ними. Европол играет ключевую роль в Европейской целевой группе по борьбе с киберпреступностью – группе экспертов в составе представителей от Европола, Евроюста и Европейской комиссии, действующих совместно с руководителями учрежденных в Европейском союзе подразделений по борьбе с киберпреступностью в целях содействия трансграничной борьбе с преступлениями в Интернете. Европол предлагает государствам – членам Европейского союза поддержку в решении проблем, связанных с киберпреступностью, а именно:

- базу данных по киберпреступности: Европол оказывает государствам – членам Европейского союза поддержку в проведении касающихся киберпреступности расследований и анализа и способствует трансграничному сотрудничеству и обмену информацией;

[147] См. www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

[148] Ibid.

- в документе "Оценка связанных с использованием Интернета угроз со стороны организованной преступности" (iOCTA) дается оценка текущих и будущих тенденций в области киберпреступности, включая террористическую деятельность и атаки на электронные сети; такая оценка служит основанием как для оперативной деятельности, так и для формулирования политики Европейского союза;
- в настоящее время в процессе разработки находятся Онлайновая система учета интернет-преступности (ICROS) и Форум специалистов по Интернету и судебных экспертов (IFOREX). Они позволят обеспечить централизованную координацию сообщений о преступлениях в Интернете, поступающих от компетентных органов государств – членов Европейского союза, а также станут базой технических данных и профессиональной подготовки сотрудников правоохранительных органов[149].

272. Наряду с оказанием такой поддержки, на оперативном уровне Европол активно участвует во взаимодействии с Евроюстом в создании и поддержке совместных следственных групп и предоставляет помощь государствам-членам в проведении расследований в форме предоставления аналитических рабочих файлов, координации работы по конкретным делам и организации тактических совещаний. В рамках предназначенной для проведения анализа платформы аналитических рабочих файлов хранятся поименные данные (например, информация о свидетелях, потерпевших, номерах телефонов, местах, транспортных средствах и событиях), которые подвергаются процессу динамического анализа, позволяющему выявить связи между предметами, субъектами и данными, фигурирующими в национальных запросах и расследованиях. Эти данные помечаются "кодом обработки", четко указывающим на условия использования, относящиеся к конкретному компоненту данных.

d) Евроюст

273. В рамках соответствующего мандата в функции Евроюста в области борьбы с терроризмом входят содействие обмену информацией между судебными органами различных государств-членов, которые участвуют в расследованиях и судебных процессах, связанных с терроризмом[150]; оказание помощи судебным органам государств-членов в выдаче и исполнении европейских ордеров на арест; а также содействие в осуществлении мер по проведению расследований и сбору улик, необходимых государствам-членам для уголовного преследования подозреваемых в совершении террористических преступлений (например, отбор свидетельских показаний, получение научных доказательств, проведение обысков и выемок, а также перехват сообщений). Двадцать семь национальных членов Евроюста (судей, обвинителей или полицейских должностных лиц с аналогичными компетенциями в своих соответствующих государствах-членах) базируются в Гааге, Нидерланды, и находятся в постоянном контакте с национальными органами в их соответствующих государствах-членах, которые могут обратиться за помощью Евроюста в ходе конкретных расследований или уголовного преследования по делам против террористов (например, в целях разрешения коллизии юрисдикций или содействия в сборе доказательств).

274. Евроюст также поощряет и поддерживает создание и работу совместных следственных групп путем предоставления специалистам-практикам информации и рекомендаций. Совместные следственные группы получают все более широкое признание в качестве эффективного

[149] См. "Cybercrime presents a major challenge for law enforcement", European Police Office press release, 3 January 2011. См. по адресу: www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523.

[150] Решение Совета Европейского союза 2005/671/JHA от 20 сентября 2005 года по вопросу об обмене информацией и сотрудничеству по делам, касающимся преступлений террористов, обязывает все государства-члены назначить национальных корреспондентов по вопросам терроризма, которые должны информировать Евроюст (агентство по сотрудничеству судебных органов Европейского союза) о любой террористической деятельности в своих странах с первых этапов допроса подозреваемых до этапа предъявления официального обвинения, а также с момента выдачи европейских ордеров на арест по делам о терроризме и до направления запросов о взаимной правовой помощи и вынесения приговора.

механизма для принятия ответных судебных мер против трансграничной преступности и как отвечающий необходимым требованиям форум для обмена оперативной информацией по конкретным делам, связанным с терроризмом. Национальные члены Евроюста могут участвовать в работе совместных следственных групп, действуя либо от имени Евроюста, либо в своем качестве представителей национальных компетентных органов по борьбе с терроризмом. Например, в случае когда в рамках рассматривавшегося в Дании дела о террористической деятельности органам власти Бельгии была направлена просьба о создании совместной следственной группы, в формировании такой группы из представителей национальных компетентных органов двух стран приняли участие датский и бельгийский отделы Евроюста. Евроюст также оказывает финансовую и материально-техническую помощь деятельности таких групп и служит местом пребывания постоянных секретариатов совместных следственных групп.

275. Издаваемый Евроюстом Вестник обвинительных приговоров по делам о терроризме (*Terrorism Convictions Monitor*) также имеет целью предоставить в распоряжение специалистов-практиков примеры судебных решений, вынесенных в одной стране, которые могут быть полезны в других странах, в частности в отношении толкования законодательства Европейского союза по вопросам борьбы с терроризмом. В выпуске Вестника за сентябрь 2010 года был представлен углубленный анализ двух дел, в которых фигурировали общие атрибуты, такие как участие джихадистов в совершении террористического акта, радикализация и использование Интернета[151]. Одним из этих дел, предоставленным органами власти Бельгии, было дело *Малика эль-Аруд и другие*, о котором рассказывается ниже (см. пункт 377). Группа Евроюста по борьбе с терроризмом регулярно проводит совещания тактического и стратегического характера, посвященные тенденциям эволюции терроризма, в ходе которых ведущие судьи и эксперты по правовым аспектам борьбы с терроризмом из Европейского союза и стран, не входящих в Европейский союз, делятся своим опытом по конкретным вопросам. К числу примеров таких встреч можно отнести состоявшееся в 2010 году стратегическое совещание по вопросам использования VoIP-технологий в террористических целях и необходимости законного перехвата сообщений, а также проведенное в апреле 2011 года тактическое совещание, посвященное основанным на насилии и выступающим единым фронтом экстремизму и терроризму. На этих совещаниях выявляются общие проблемы, а также распространяется передовой опыт и соответствующие знания среди лиц, определяющих политику Европейского союза, в целях определения возможных способов придания большей эффективности координации борьбы с терроризмом.

C. Национальные законодательные рамки

276. Одним из основополагающих элементов структуры, способствующей действенному международному сотрудничеству в расследовании и уголовном преследовании по делам о терроризме, является наличие на национальном уровне законодательных рамок для осуществления международного сотрудничества. Посредством такого законодательства принципы международного сотрудничества, закрепленные в универсальных документах по борьбе с терроризмом, должны быть включены во внутреннее законодательство страны.

277. Наряду с выпуском ряда публикаций, которые призваны помочь странам включить механизмы международного сотрудничества в свое законодательство, в перечень услуг, предоставляемых Сектором ЮНОДК по вопросам предупреждения терроризма в целях содействия странам в выполнении их международных обязательств по борьбе с терроризмом, входят оказание консультативной поддержки, обучение персонала и создание потенциала в данных областях.

[151] *Terrorism Convictions Monitor* можно получать, направив запрос в Группу Евроюста по борьбе с терроризмом.

D. Меры, не связанные с законодательством

278. Хотя присоединение к многосторонним и двусторонним документам и принятие соответствующего законодательства являются основными компонентами любого эффективного режима международного сотрудничества, они не дают исчерпывающего ответа на проблему. Одним из ключевых элементов успешной организации эффективного международного сотрудничества является наличие обеспеченного соответствующими ресурсами и действующего на опережение центрального органа, способного, опираясь на любые доступные механизмы (как официальные, так и неофициальные), оказать своевременную и действенную поддержку в развитии сотрудничества.

279. Важной предпосылкой успешного международного сотрудничества является наличие эффективной межведомственной координации между правоохранительными органами, специализированными разведывательными ведомствами (например, подразделениями финансовой разведки) и центральными органами власти на национальном уровне, подкрепляемой необходимым законодательством и четкими, отвечающими современным требованиям процедурами обработки запросов.

280. Удачным примером сотрудничества как на национальном, так и на международном уровне является следующее дело, которое велось в Колумбии и в рамках которого имело место широкое официальное и неофициальное сотрудничество между компетентными органами.

Дело в отношении Революционных вооруженных сил Колумбии (ФАРК)

1 марта 2008 года колумбийские вооруженные силы провели ряд операций против предполагаемых членов Революционных вооруженных сил Колумбии (ФАРК). В ходе этих операций одно лицо, подозревавшееся в том, что оно являлось одним из руководителей ФАРК, и несколько других членов организации были убиты; кроме того, были собраны улики, в число которых входили электронные устройства, такие как компьютеры, электронные ежедневники и USB-накопители. Предметы, содержавшие цифровые улики, были переданы колумбийской судебной полиции для использования в процессе возможных уголовных расследований и при возбуждении судебных дел.

Извлеченные с цифровых устройств данные помогли выявить информацию о существовании международной сети поддержки данной организации, в том числе о связях в ряде стран Центральной и Южной Америки и Европы. Основными целями этой сети являлись сбор средств на финансирование деятельности ФАРК, вербовка новых членов и пропаганда политики организации, в том числе удаление названия организации из различных перечней террористов, которые ведутся в Европейском союзе и некоторых других странах. На основе полученных доказательств государственный обвинитель Колумбии возбудил в отношении лиц, подозревавшихся в поддержке и финансировании ФАРК, уголовное расследование.

Улики, которыми компетентные органы Колумбии поделились с коллегами из Испании, помогли выявить руководителя отделения ФАРК в Испании, известного под псевдонимом Леонардо. Леонардо въехал в Испанию в 2000 году и получил политическое убежище.

Государственный обвинитель Колумбии получил достаточные доказательства, чтобы распорядиться об издании в отношении Леонардо ордера на арест в целях его экстрадиции, и, используя дипломатические и иные каналы международного правового сотрудничества, затребовал его выдачи в Колумбию для предания суду.

Леонардо был арестован в Испании, а в ходе обысков по месту его жительства и работы были обнаружены документы и электронные устройства, содержавшие доказательства его причастности к расследуемым преступлениям. Впоследствии он был освобожден под залог; его незамедлительной выдаче помешал его статус беженца.

В Колумбии против Леонардо было заочно возбуждено уголовное дело в связи с его предполагаемой причастностью к финансированию терроризма. Решением Верховного суда Колумбии информация, полученная в ходе операции 1 марта 2008 года и находившаяся на изъятых электронных устройствах, была признана недопустимой. Впоследствии государственный обвинитель, совместно с коллегами из ряда других стран, в которых имелись члены сети поддержки ФАРК, использовал все доступные каналы международного сотрудничества для выявления членов данной сети в Испании и других европейских странах и сбора дополнительных доказательств в поддержку судебного дела.

Кроме того, в ответ на полученное от государственного обвинителя Колумбии поручение судебные власти Испании передали своим колумбийским коллегам всю информацию, которая была собрана в ходе полицейских рейдов и обысков в доме Леонардо. По данным испанской судебной полиции, эта информация подтверждала виновность Леонардо и других лиц в создании на территории Испании террористической ячейки ФАРК. Она также помогла установить виновность Леонардо в финансировании терроризма и укрепила подозрение о возможном существовании связи между Леонардо и лицами, привлеченными к уголовной ответственности за их связи с террористической группой Euskadi Ta Askatasuna (ЭТА) ("Страна басков и свобода"). В результате проведенных в Испании обысков были изъяты дополнительные документальные и цифровые доказательства, по существу сходные с доказательствами, которые были признаны недопустимыми. Опираясь на эти новые доказательства, предоставленные компетентными органами Испании, колумбийский государственный обвинитель продолжил судебное разбирательство в отношении Леонардо. Кроме того, благодаря новым доказательствам удалось установить, что со стороны ФАРК предпринимались усилия по обеспечению своим членам доступа в университеты, неправительственные организации и иные государственные учреждения, в которых можно было бы найти возможности финансирования и вербовки новых членов.

Эти доказательства также подтвердили существование в ФАРК "международной комиссии", управляющей программой обеспечения безопасности сообщений, в частности передаваемых через Интернет или по радио (постоянные средства связи между руководством организации и членами международной сети поддержки), путем шифрования передаваемой информации, использования стеганографии для сокрытия сообщений, рассылки спама по электронной почте и удаления истории доступа к ресурсам сети, чтобы гарантировать, что информация не попадет в руки следователей или судебных органов. В связи с этим испанские и колумбийские компетентные органы наладили сотрудничество в целях "взлома" ключей и расшифровки сообщений, передававшихся предполагаемыми руководителями ФАРК в Колумбии и Испании.

Прежде чем начать уголовный процесс против Леонардо, государственный обвинитель Колумбии обратился к судье с просьбой рассматривать новые улики как "доказательства, полученные позднее" и из "независимого источника". Результатом этого обращения, которое было удовлетворено, стало разрешение включить эти доказательства в процесс судебного производства без создания оснований, по которым в противном случае подобные доказательства не были бы допущены.

В настоящее время судебный процесс в Колумбии по делу обвиняемого в финансировании терроризма подсудимого Леонардо продолжается заочно в ожидании результатов рассмотрения дела о его выдаче.

281. В рамках описанного выше дела компетентные органы воспользовались как официальными механизмами взаимной правовой помощи, так и своими неформальными связями. Хотя объемы взаимной помощи, которая может быть оказана компетентными органами разных стран в отсутствие договора или соответствующего официального запроса, могут различаться, в случае связанных с терроризмом расследований компетентные органы многих стран в той или иной мере располагают возможностями оказания помощи на основании неофициальных запросов от зарубежных коллег. На совещании группы экспертов был отмечен ряд случаев и обстоятельств, при которых такое неофициальное сотрудничество было или могло быть использовано для успешного расследования дел, связанных с использованием Интернета террористами.

1. Важность поддержания связей

282. На оперативном уровне также крайне важно, чтобы национальные органы охраны правопорядка и уголовного преследования поощряли, устанавливали и поддерживали доверительные отношения с зарубежными коллегами, с которыми им, возможно, предстоит сотрудничать при проведении трансграничных уголовных расследований.

283. Учитывая по большей части транснациональный характер террористической и связанной с ней преступной деятельности, чрезвычайно сложный и деликатный характер расследований, проводимых на основе разведывательной информации, а также необходимость безотлагательных действий в условиях быстро меняющихся обстановки и хода следствия, доверие между органами охраны правопорядка и уголовного преследования как на национальном, так и на международном уровне нередко становится решающим фактором успешного расследования преступлений, связанных с терроризмом, и судебного преследования за их совершение. Это особенно важно в контексте Интернета, когда сохранение, например, данных об использовании и цифровых улик, содержащихся в компьютерах и других портативных устройствах, нередко находящихся не в одной, а в нескольких различных юрисдикциях, часто является критически важным доказательством на судебном процессе и должно быть осуществлено в самые сжатые сроки. Личные контакты с коллегами в других юрисдикциях, знакомство с их процессуальными нормами и доверие являются факторами, способствующими эффективному международному сотрудничеству.

284. Хотя средства, позволяющие осуществлять неофициальное сотрудничество в конкретных странах, могут быть различными, отдельные элементы установившейся практики оказания неофициальной помощи при связанных с терроризмом расследованиях все же можно определить.

a) Создание эффективных механизмов для обмена информацией: использование офицеров связи

285. На заседании экспертной группы некоторые специалисты отмечали, что их национальные правоохранительные ведомства располагают сетями международных пунктов связи, которые оказывают значительную помощь, содействуя выполнению запросов о международном сотрудничестве. Например, Федеральное управление уголовной полиции Германии (Bundeskriminalamt) имеет офицеров связи и поддерживает прямые контакты в 150 странах. Кроме того, созданная в 2007 году Европейская экспертная сеть по вопросам терроризма объединяет специалистов из научных учреждений, полиции и разведывательных служб и оказалась весьма эффективным каналом для обмена информацией и опытом между ее членами на междисциплинарной основе.

286. Дело *Государство против Намуха* является примером в высшей степени успешного международного сотрудничества между органами охраны правопорядка/уголовного преследования Австрии и Канады, осуществлявшегося исключительно на неофициальной основе, в ходе расследования и уголовного преследования в отношении лиц, находившихся в этих

юрисдикциях и участвовавших в связанной с терроризмом деятельности с использованием Интернета.

Государство против Саида Намуха

Г-н Саид Намух являлся подданным Марокко, проживавшим в небольшом городке в Канаде.

10 марта 2007 года на одном из веб-сайтов в Интернете был размещен видеоролик с записью "открытого" письма, которое читал шейх Айман аз-Завахири. В нем аз-Завахири предупреждал правительства Австрии и Германии, что они должны вывести свои войска из состава миссии по поддержанию мира в Афганистане, в противном случае они будут нести ответственность за последствия. Аз-Завахири заявлял в своем послании:

> Мир – это дело обоюдное. Если будем в безопасности мы, будете в безопасности и вы. Будем жить в мире мы, будет мир и у вас, но если вы намерены нас убивать, то, даст Бог, разбиты и убиты будете вы. Это точное уравнение. Так попытайтесь же это понять, если вы способны что-либо понимать.

Фоном для видео с сопроводительными комментариями аз-Завахири служила мозаика из изображений, в том числе бронеавтомобилей с национальными флагами и видных австрийских и немецких государственных деятелей. В отдельных частях видео фигурировали фотографии аз-Завахири и других лиц, скрытых капюшонами.

После трансляции этого видео компетентные органы Австрии начали расследование, в рамках которого велся перехват различных сообщений, передававшихся проживавшим в Вене австрийским гражданином Мохаммедом Махмудом. Эти сообщения включали проводившиеся на арабском языке переговоры с использованием интернет-телефонии и обмены информацией в чат-форумах, которые показали, что г-н Махмуд поддерживал связь с неким лицом, находившимся в Канаде, по вопросам, связанным с джихадом, в том числе с планированием террористического акта, скорее всего в Европе. Участники обсуждали возможность использования взрывчатых веществ и другие мероприятия в связи с нападением.

В результате мероприятий по перехвату было установлено, что одним из участников вышеуказанных обменов сообщениями был проживавший в Канаде Саид Намух. В июле 2007 года к проведению расследования, координация которого между австрийскими и канадскими компетентными органами осуществлялась базировавшимся в Вене офицером связи правоохранительных органов Канады, присоединилась Королевская канадская конная полиция. Хотя между Австрией и Канадой существовал официальный договор о взаимной правовой помощи, никаких формальных запросов об оказании взаимной правовой помощи на основании этого договора не направлялось; сотрудничество осуществлялось исключительно на неофициальной основе.

Расследование показало, что в период с ноября 2006 года по сентябрь 2007 года некое лицо, пользовавшееся интернет-подключением г-на Намуха, проводило в Интернете значительное количество времени и постоянно поддерживало контакты с адептами джихада во всем мире, в том числе через Глобальный исламский информационный фронт (ГИИФ), одну из старейших и наиболее известных виртуальных групп джихадистского толка. Опираясь на поддержку центра "Аль-Фаджр", ГИИФ выступает в качестве информационного крыла "Армии ислама" [Джейш аль-Ислам]. Среди прочего ГИИФ распространяет пропагандистские материалы и обеспечивает джихадистов инструментарием (например, руководствами по применению взрывных устройств, программным обеспечением для шифрования), необходимым для ведения джихада. Значительная часть деятельности г-на Намуха в Интернете была связана с размещением сообщений на различных форумах, часто посещаемых джихадистами.

В мае 2007 года бойцами "Армии ислама" в Газе был похищен журналист Би-би-си Алан Джонстон. ГИИФ опубликовал в связи с этим событием несколько видеоматериалов, однако особого внимания заслуживали опубликованные 9 мая 2007 года видеоматериалы, в которых "Армия ислама" взяла на себя ответственность за похищение, а также видеоматериалы, опубликованные 20 и 25 июня, в которых содержались угрозы казнить журналиста, если определенные требования не будут удовлетворены. К счастью, г-н Джонстон был освобожден целым и невредимым 3 июля 2007 года.

7 и 8 мая сообщения, посланные г-ном Намухом через чат-форум в Интернете и перехваченные компетентными органами, показали, что г-н Намух участвовал в дискуссиях, касавшихся похищения Алана Джонстона, и конкретно в обсуждениях, связанных с подготовкой опубликованного несколько позже – 9 мая – сообщения ГИИФ о своей ответственности за похищение. Согласно расшифровке содержания интернет-чата от 8 мая, представленной в суде в качестве доказательства (в переводе с арабского языка на французский), г-н Намух писал: "Мой возлюбленный брат Абу Обаяда, оставайся на линии с нами, и да ниспошлет тебе Аллах сокровище, которое позволит тебе увидеть, что надлежит делать; Бог даст, заявление будет сделано сегодня".

Всего за период с 3 июня по 9 сентября 2007 года между Намухом и Махмудом состоялась 31 беседа. Эти беседы показали, что они планировали осуществить взрыв в неустановленном месте в Европе и обсуждали способы получения или изготовления начиненного взрывчаткой "пояса шахида", вопросы финансирования и планы поездок для встреч с другими лицами в странах Магриба и Египте в целях завершения приготовлений. Эти разговоры указывали на то, что предположительно террористом-смертником должен был стать г-н Намух.

12 сентября 2007 года, опасаясь, что эти планы были очень близки к осуществлению, компетентные органы в Австрии и Канаде одновременно произвели аресты Намуха и Махмуда.

В Канаде г-ну Намуху были предъявлены обвинения в сговоре в целях применения взрывчатых веществ (в неустановленном месте в Европе), участии в деятельности террористической группы, содействии террористической деятельности и шантажировании иностранного правительства (видео с угрозами в отношении Австрии и Германии).

На суде защита г-на Намуха оспорила ряд аспектов обвинения, в том числе выдвинув на основании конституционных норм доводы, касавшиеся права на свободу выражения мнения (в связи с вопросом о том, является ли ГИИФ террористической организацией). Были высказаны возражения в отношении объективности главного свидетеля-эксперта, вызванного обвинением для дачи показаний о движении "Аль-Каида", его ответвлениях, глобальном джихадизме (в том числе о виртуальном джихадизме) и методах и стиле пропагандистской деятельности ГИИФ, а также об использовании этой организацией Интернета. Защита также оспаривала, можно ли считать терроризмом деятельность, проводимую ГИИФ и связанными с ним группами, а также достоверность доказательств, основанных на перехвате передававшихся через Интернет сообщений в Австрии и Канаде, и точность перевода записей этих сообщений с арабского на французский язык. Защита обратилась к суду с просьбой постановить, что различные сообщения, распространявшиеся г-ном Намухом от имени ГИИФ, следует воспринимать фигурально, а не как акты консультирования в отношении совершения актов терроризма или поощрения к их совершению.

При рассмотрении доводов защиты в отношении характера материалов, размещавшихся или передававшихся от имени ГИИФ, суд пришел к следующему заключению:

> По данному вопросу у Суда нет никаких сомнений. Контекст этих сообщений явно указывает на реальные действия, поощряемые ГИИФ. Повсюду сеются смерть и разрушения. Пропагандируемый ГИИФ джихад основан на насилии. Эта пропаганда безусловно представляет собой консультирование ("поощрение"), а иногда и угрозу совершения террористических действий. Таким образом, эта деятельность бесспорно подпадает под определение террористической деятельности по смыслу статьи 83.01 Уголовного кодекса.

Признавая г-на Намуха виновным в консультировании или поощрении к совершению террористических актов, суд сослался на перехваченные сообщения, в которых содержались заявления, свидетельствовавшие о ревностном, активном характере его участия в деятельности ГИИФ. Кроме того, релевантным, по мнению суда, был ряд сообщений, включая приводимое ниже сообщение от 12 декабря 2006 года, в котором подсудимый выражал желание скрыть свою деятельность, а также деятельность ГИИФ путем удаления инкриминирующих компьютерных данных:

> [ПЕРЕВОД]
> Срочно Срочно Срочно
> Да пребудут с тобой мир, милость и благословения Аллаха.
> Я хочу стереть все хранящиеся на моем компьютере джихадистские фильмы и книги, не оставляя никаких следов, да благословит тебя Аллах, потому что, как я подозреваю, кто-то проверяет мой компьютер.
> Да пребудут с тобой мир, милость и благословения Аллаха.

В других сообщениях подсудимый интересовался использованием анонимизирующего программного обеспечения и аналогичных средств, которые можно использовать для сокрытия своей деятельности. После состоявшегося в октябре 2009 года суда подсудимый был признан виновным по всем пунктам обвинения; позже он был приговорен к пожизненному заключению.

b) Совместные расследования

287. Хотя понятие "совместные расследования" упоминается в ряде международных договоров (например, в статье 19 Конвенции Организации Объединенных Наций против транснациональной организованной преступности), в универсальных документах по борьбе с терроризмом прямых ссылок на такую стратегию не содержится. Тем не менее такой подход к расследованиям полностью отвечает основополагающим принципам и духу закрепленных в данных документах элементов международного сотрудничества. В некоторых странах, особенно в Европе, этот подход успешно применяется в ходе ряда расследований, связанных с терроризмом, и следует отметить, что важная роль в создании и поддержке совместных следственных групп принадлежит Европолу. Основной задачей таких совместных следственных групп, в состав которых входят как служащие национальных правоохранительных органов, так и сотрудники Европола, является проведение расследований, имеющих конкретные цели и ограниченных по срокам, в одном или нескольких государствах-членах[152].

288. Европол работает совместно с системой национальных подразделений, состоящей из назначаемых для поддержания контактов групп в рамках национальных полицейских сил. Он содействует и поощряет обмен информацией между государствами-членами через защищенную цифровую сеть и предоставляет в их распоряжение систему из 17 аналитических рабочих

[152] Eveline R. Hertzberger, *Counter-Terrorism Intelligence Cooperation in the European Union* (Turin, Italy, United Nations Interregional Crime and Justice Research Institute, July 2007).

файлов, составляющую правовую базу Европола, предназначенную в первую очередь для обеспечения полноценной координации и сотрудничества между участвующими компетентными органами.

289. Хотя на международном уровне достаточно трудно оценить, насколько активно страны пользуются такого рода сотрудничеством, дискуссии на совещании группы экспертов показали, что в рамках ответственных за обеспечение правопорядка и безопасности международных сообществ растет осознание того, что, с учетом характера современного терроризма и способов действий террористов, тесное сотрудничество при расследовании дел о терроризме становится все более важным компонентом успешных усилий по пресечению и предупреждению террористических актов и уголовному преследованию за их совершение.

E. Официальное сотрудничество в сравнении с неофициальным

290. Международное сотрудничество в связи с делами о терроризме, задействующее трансграничный элемент, может принимать самые разные формы в зависимости от характера расследуемого преступления, вида запрашиваемой помощи, применимого национального законодательства, а также наличия и статуса любых договоров или соглашений в поддержку такого сотрудничества.

291. Хотя общий уровень действенности и эффективности формальных процедур оказания взаимной правовой помощи по уголовным делам повысился, они по-прежнему могут быть достаточно длительными и требовать значительного объема бюрократических усилий со стороны как запрашивающих, так и запрашиваемых стран. Во многих делах о терроризме, особенно связанных с совершением преступлений в Интернете, неофициальное сотрудничество все чаще оказывается столь же важным, что и сотрудничество по официальным каналам, позволяя избегать значительных задержек в ситуациях, когда срочные действия (например, по обеспечению сохранности данных о пользовании Интернетом) играют центральную роль в обеспечении успешного исхода судебного преследования. Участники совещания группы экспертов указали на важность перспективного развития и использования, когда это возможно, национальными разведывательными и правоохранительными органами, а также органами обвинения доступных механизмов содействия международному сотрудничеству как по неофициальным, так и по официальным каналам.

292. Во многих случаях, например когда компетентные органы одной страны стремятся обеспечить сохранность интернет-данных, находящихся у провайдера услуг Интернет в другой стране, эти органы могут прибегнуть к неофициальному сотрудничеству в целях сохранения таких данных для их использования в процессе расследования или судебного преследования в связи с совершением уголовного преступления.

293. Правовые вопросы в рамках проведения уголовных расследований, связанных с Интернетом, в частности вопросы, касающиеся юрисдикции, могут быть крайне сложными. В случаях, когда следователям в одной стране нужно получить доступ к информации, хранящейся на компьютерах, которые находятся в другой стране, могут возникнуть сложные вопросы в отношении юридических правомочий и оснований для действий этих следователей. Хотя компетентные органы одной страны вполне могут обратиться непосредственно к тем сторонам в другой стране, которые располагают разыскиваемой ими информацией, ответы на такое обращение могут быть различными. Как правило, желательно, чтобы для получения такой информации компетентные органы сотрудничали со своими зарубежными коллегами, по возможности на неофициальной основе.

294. Формы и методы сотрудничества во многом будут зависеть от характера и назначения запрашиваемой помощи. Например, компетентные органы одной страны, возможно, вправе оказать неофициальную помощь зарубежным коллегам, потребовав от провайдеров услуг

Интернет добровольно сохранить данные, связанные с Интернетом, однако для проведения обыска и изъятия таких данных, как правило, требуется разрешение суда, которое может быть получено только официальным путем.

295. Иногда официальный запрос является единственным способом, позволяющим компетентным органам предоставить запрашиваемое взаимное сотрудничество. В таких случаях важно, чтобы в странах действовали законодательство и процедуры, предусматривающие своевременное и эффективное реагирование на запросы, для того чтобы, насколько это возможно, максимально повысить вероятность успеха такой помощи.

Неофициальное сотрудничество

296. Учитывая потенциальную важность и срочность обнаружения и обеспечения сохранности связанных с Интернетом данных при расследовании дел о терроризме, а также вероятность того, что такая информация будет находиться в другой стране, следователи должны рассматривать возможность использования как официальных, так и неофициальных путей ее получения. Использование официальных каналов взаимной правовой помощи может обеспечить бóльшую определенность в решении связанных с ней правовых вопросов, но это также требует больше времени и сопряжено с бóльшим числом бюрократических процедур, чем использование неофициальных каналов.

297. На совещании группы экспертов специалист из Канады подчеркнул решающую роль в обеспечении успешного исхода судебного преследования, которую сыграло тесное неофициальное сотрудничество между Королевской канадской конной полицией и австрийским Федеральным агентством по защите государства и борьбе с терроризмом (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung), осуществлявшееся при содействии базировавшегося в Вене канадского офицера связи. Помимо этого дела, другие эксперты также приводили аналогичные примеры, когда использование офицеров связи для содействия неофициальному сотрудничеству играло важную роль в достижении успешных результатов.

298. Связанные с Интернетом данные, такие как хранящаяся у провайдеров сетевых услуг информация об использовании Интернета их клиентами, как правило, служат решающими доказательствами по делам о терроризме, связанным с использованием компьютеров и Интернета. Если следователям удается физически завладеть компьютерами, которые использовали подозреваемые, а также получить связанные с их использованием данные, которые хранились провайдерами услуг Интернет, у них оказывается больше шансов установить связь подозреваемого с совершенным преступлением.

299. Принимая во внимание это обстоятельство, следователям и обвинителям важно в полной мере учитывать потенциальную важность связанных с Интернетом данных и необходимость как можно скорее принять меры к их сохранению таким образом, чтобы была гарантирована их допустимость в качестве потенциальных доказательств в ходе любого последующего судебного разбирательства. По мере возможности, национальным правоохранительным органам следует выработать, либо непосредственно с провайдерами услуг Интернет, либо с коллегами в компетентных органах других стран, четкие процедуры с использованием как официальных, так и неофициальных элементов, направленные на обеспечение как можно более срочного сохранения и предоставления необходимых для уголовного расследования данных об использовании Интернета.

300. В Соединенных Штатах, где находятся многие крупнейшие провайдеры услуг Интернет, компетентные органы применяют "двойной" подход к оказанию содействия зарубежным коллегам в сохранении и предоставлении для возможного использования в доказательных целях связанных с Интернетом данных, которые хранятся у провайдеров услуг Интернет, базирующихся в Соединенных Штатах. В рамках такого подхода возможны два метода обработки зарубежных запросов о сохранении и предоставлении имеющейся у провайдеров услуг Интернет информации об учетных записях пользователей.

a) *Неофициальная процедура.* Существуют два способа, с помощью которых следственные органы могут обеспечить сохранение находящихся в Соединенных Штатах данных, связанных с Интернетом, неофициальными средствами: i) иностранные компетентные органы могут вступить в прямой контакт с провайдерами услуг Интернет и обратиться к ним непосредственно с неофициальной просьбой сохранить и предоставить необходимые данные; или ii) если такой прямой связи не существует, они могут направить неофициальный запрос через Федеральное бюро расследований, которое обратится с соответствующим требованием к провайдеру услуг Интернет.

b) *Официальная процедура.* В рамках официальной процедуры компетентные органы иностранных государств могут обратиться с официальным запросом о предоставлении взаимной правовой помощи в отношении данных, касающихся учетной записи конкретного пользователя, который будет обработан в Управлении по международным вопросам Министерства юстиции Соединенных Штатов. По получении запрос подлежит рассмотрению в Отделе по борьбе с терроризмом этого Министерства в целях установления, не связан ли он с каким-либо расследованием, ведущимся в Соединенных Штатах. Если нет, то запрос направляется в федеральный суд для получения необходимого предписания с разрешением осуществить сбор требуемой информации и ее передачу компетентным органам запрашивающей страны.

301. Вышеописанный порядок предоставления данных, связанных с провайдерами услуг Интернет, успешно применялся в ходе ряда расследований по делам о терроризме, которые проводили компетентные органы Соединенного Королевства и Соединенных Штатов. В одном конкретном случае в результате применения этой процедуры от базирующегося в Соединенных Штатах провайдера услуг Интернет был получен существенный объем кешированных интернет-данных, которые стали важнейшей уликой на проходившем в Соединенном Королевстве уголовном процессе.

F. Проблемы и спорные вопросы

302. По самой своей природе связанные с Интернетом виртуальная географическая зона покрытия, фрагментированная структура и быстро развивающиеся технологии постоянно ставят перед правоохранительными органами и органами уголовной юстиции, участвующими в расследованиях и уголовном преследовании по делам о терроризме, трудноразрешимые задачи и проблемы. В ходе дискуссий на совещании группы экспертов обращалось внимание на ряд областей, которые в настоящее время остаются проблематичными в плане международного сотрудничества. К их числу относятся возникающие в некоторых случаях затруднения с обеспечением выполнения содержащегося в запросах о выдаче и взаимной правовой помощи критерия "двойной уголовной ответственности". Ряду экспертов приходилось сталкиваться со случаями задержек или отказов в удовлетворении запросов о взаимной правовой помощи или выдаче из-за проблем с выполнением требований в отношении "двойной уголовной ответственности". В некоторых случаях это было результатом несовместимости положений о правонарушениях уголовного порядка, а в других – следствием чрезмерно ограничительного подхода к судебному толкованию соответствующих положений о криминализации со стороны судебных органов. По мнению ряда экспертов, в связи с данной ситуацией на первый план выдвигается необходимость специальной подготовки сотрудников судебных органов по вопросам международного сотрудничества.

1. Защита секретной информации

303. На совещании группы экспертов специалисты из ряда стран упоминали о проблемах, постоянно возникающих в связи с обменом конфиденциальной разведывательной информацией, который осуществляется национальными правоохранительными органами и разве-

дывательными службами с зарубежными коллегами. Уголовные расследования и судебное преследование по делам о терроризме неизменно ведутся на основе разведывательных данных, по крайней мере на ранних стадиях, и связаны с привлечением тщательно охраняемой и защищаемой секретной информации. Раскрытие такой информации сопряжено со значительными рисками, часто не только для источника ее происхождения, но и для владеющего ею ведомства или ведомств, особенно если раскрытие информации создает вероятность или возможность компрометации текущего или будущего расследования или операции.

304. Проведение компетентными национальными органами оценок того, целесообразно ли делиться такой информацией, при каких обстоятельствах или на каких условиях, может быть сложным делом, требующим от них рассмотрения ряда факторов. Тем не менее, независимо от конкретных критериев, которые применяются для оценки возможности обмена информацией, во всех случаях, каковы бы ни были обстоятельства, раскрывающее информацию ведомство обязательно должно убедиться в том, что, получив ее в свое распоряжение, принимающее ведомство будет обеспечивать согласованные гарантии и защиту предоставленных сведений.

2. Суверенитет

305. Концепция суверенитета, включая право народов на определение собственного политического статуса и осуществление неотъемлемого суверенитета в пределах своей территориальной юрисдикции, является общепризнанным принципом межгосударственных отношений и международного права. Дела, требующие расследования или уголовного преследования в связи с трансграничной деятельностью террористов или других преступников, могут быть сопряжены с определенными последствиями для суверенитета тех стран, в которых должны проводиться такие расследования.

306. В ряде случаев опасения, оправданные или нет, которые испытывают национальные органы власти в отношении того, что́ воспринимается ими как нарушение их государственного суверенитета, могут препятствовать эффективному международному сотрудничеству по уголовным делам. Поэтому важно, чтобы, обдумывая возможные следственные действия, которые предполагают сбор доказательств, связанных с компьютерами и Интернетом, следователи и обвинители не забывали о вероятных последствиях, которые такие следственные действия могут иметь для суверенитета других государств (например, когда компетентные органы одной страны проводят дистанционный обыск компьютера, используемого подозреваемым, находящимся в другой стране).

307. Вообще говоря, когда это возможно, планируя следственные действия в отношении лиц или предметов, находящихся на территории другой юрисдикции, национальным компетентным органам следует уведомить об этом своих зарубежных коллег в соответствующих странах и осуществлять такие действия в координации с ними.

3. Хранение и производство данных, относящихся к Интернету

308. Как уже отмечалось, во многих делах о терроризме значительная часть улик против подозреваемых правонарушителей неизбежно оказывается сопряженной с теми или иными аспектами связанной с Интернетом деятельности подозреваемого (например, информация о выставлении счетов по кредитным картам, данные об использовании клиентом средств связи, основанных на интернет-технологиях, таких как электронная почта, VoIP, Skype, или сведения, относящиеся к социальным сетям или другим веб-сайтам). Во многих случаях следственным органам оказывается необходимо обеспечить хранение относящихся к делу интернет-данных и их сохранность для последующего использования в качестве доказательств в ходе судебного процесса. В связи с этим важно отметить различие между "хранением" данных и их "сохранностью". Во многих странах провайдеры услуг Интернет по закону обязаны хранить определенные виды данных в течение указанного периода времени. С другой

стороны, сохранность данных означает обязательство, налагаемое на провайдера услуг Интернет согласно приказу, предписанию или распоряжению суда в целях обеспечения сохранения данных в указанных условиях для предъявления в качестве доказательств в ходе уголовного судопроизводства.

309. Одной из главных проблем, стоящих перед всеми правоохранительными органами, является отсутствие согласованного на международном уровне режима хранения данных, находящихся у провайдеров услуг Интернет. В то время как правительства многих стран возложили на базирующихся в них провайдеров услуг Интернет юридические обязательства хранить связанные с Интернетом данные для нужд правоохранительных органов, на международном уровне не существует единого общепризнанного стандартного срока, в течение которого каждый провайдер услуг Интернет обязан хранить соответствующую информацию.

310. В результате в то время как в тех странах, в которых на провайдеров услуг Интернет возложены определенные обязательства по хранению данных, следователи, занимаясь чисто внутренними расследованиями, могут быть в какой-то степени уверены относительно типа интернет-данных и того, как долго они будут сохраняться провайдерами услуг Интернет, этого нельзя сказать о расследованиях, в ходе которых возникает необходимость собрать данные, хранящиеся у провайдеров услуг Интернет в других странах.

311. В Соединенных Штатах в рамках нынешнего подхода от провайдеров услуг Интернет требуется хранить данные об использовании по конкретным запросам правоохранительных органов, тогда как сами провайдеры услуг Интернет применяют самые разные правила в отношении периода хранения данных: от нескольких дней до нескольких месяцев.

312. Несмотря на усилия, особенно заметные в рамках Европейского союза, оказалось, что достичь какого-то единообразия в этом вопросе, даже на уровне Европейского союза, весьма проблематично. В соответствии с Директивой 2006/24/ЕС Европейского парламента и Совета Европейского союза от 15 марта 2006 года о хранении данных, генерируемых или обрабатываемых в связи с предоставлением общедоступных услуг электронного обмена данными или сетей связи общего пользования, изменяющей Директиву 2002/58/ЕС, при решении вопросов о хранении данных, которые находятся у провайдеров услуг электронного обмена данными и сетей связи общего пользования, государства – члены Европейского союза обязаны обеспечивать, чтобы провайдеры, деятельность которых регламентируется, хранили указанные данные о передаче информации в течение периода от шести месяцев до двух лет. Однако, невзирая на эту Директиву, единого твердого срока хранения данных для всех базирующихся на территории Европейского союза провайдеров услуг Интернет по-прежнему не существует и эти сроки широко варьируются в предусмотренном в Директиве диапазоне от шести месяцев до двух лет. Соответственно, хотя в этих вопросах наблюдается бóльшая определенность, даже в рамках Европейского союза существуют различия в сроках хранения данных базирующимися там провайдерами услуг Интернет.

313. Несколько участников совещания группы экспертов придерживались мнения, что значительную пользу правоохранительным и разведывательным органам, расследующим дела о терроризме, принесла бы разработка общепризнанной нормативной базы, согласно которой на всех провайдеров услуг Интернет налагались бы единообразные обязательства в отношении типов подлежащих сохранению данных об использовании их услуг клиентами, а также длительности их хранения.

314. Учитывая отсутствие общепризнанных стандартов или возлагаемых на провайдеров услуг Интернет и провайдеров других коммуникационных услуг обязательств в отношении хранения связанных с Интернетом данных, при проведении уголовных расследований важно, чтобы следователи и обвинители уже на самом раннем этапе установили, существуют ли такие данные и в течение какого периода они будут сохраняться, вероятно ли, что они могут

представить интерес для стороны обвинения, и где они находятся, а также применимые временные рамки, если таковые имеются, в течение которых сторона, владеющая этими данными, обязана их хранить. В случае возникновения сомнений представителям компетентных органов было бы целесообразно связаться со своими коллегами в стране, в которой находятся данные, и предпринять шаги (по официальной или неофициальной линии), которые могут потребоваться в целях обеспечения сохранности информации для возможного предъявления ее суду. В зависимости от обстоятельств, в том числе от знакомства с соответствующим провайдером услуг Интернет или наличия связей с ним, компетентные органы могли бы рассмотреть возможность вступления в прямой контакт с таким провайдером и неофициального обращения к нему за помощью. Однако, принимая во внимание деликатный характер вопросов сохранения конфиденциальности информации клиента и соблюдения национальных законов о неприкосновенности частной жизни граждан, уровень "отзывчивости" провайдеров услуг Интернет на подобные прямые неофициальные просьбы может значительно различаться. В целях обеспечения сохранности и предоставления такой информации следователям и обвинителям всегда было бы разумно поддерживать связь и координировать усилия со своими зарубежными коллегами.

4. Требования в отношении предъявления доказательств

315. Для того чтобы свидетельские показания, вещественные доказательства или иная информация были допустимы в качестве доказательств по уголовному делу в суде, следователям и обвинителям надлежит с большой тщательностью следить за тем, чтобы используемые при их сборе, сохранении, предъявлении или передаче методы находились в полном соответствии с применимыми законами, правовыми принципами и нормами доказательственного права. Несоблюдение требований, касающихся допустимости доказательств, может привести к ослаблению версии обвинения вплоть до того, что компетентные органы, возможно, даже будут вынуждены прекратить соответствующее дело или отказаться от обвинения. В деле Намуха канадские обвинители сумели обеспечить, благодаря тесному взаимодействию со своими австрийскими коллегами, чтобы существенно важные доказательства относительно использования подсудимым чат-форумов и веб-сайтов в Интернете были собраны и переданы для использования в Канаду в допустимой форме, даже невзирая на различия действующих в этих двух странах правил доказывания.

316. В связи с делами о терроризме возникает ряд вопросов, которые могут создавать компетентным органам существенные проблемы в плане обеспечения допустимости некоторых видов информации. Их успешное преодоление остается постоянной проблемой для всех специалистов-практиков, участвующих в расследованиях и уголовном преследовании по делам о терроризме, которые нередко имеют особенности, способные воспрепятствовать допустимости информации. Транснациональный характер дел о терроризме, в том числе широкое использование разведывательной информации (нередко предоставленной иностранными партнерами на весьма жестких условиях) или узкоспециализированных, зачастую скрытых и интрузивных, методов проведения обысков, наблюдения и перехвата в качестве основы для сбора доказательств, может стать для компетентных органов значительным препятствием при попытке представить допустимые доказательства в суде или трибунале.

317. В контексте дел о терроризме, если говорить конкретно о проблемах с предъявлением доказательств, которые могут возникать в связи с Интернетом или компьютерными технологиями, то общий подход со стороны следователей и обвинителей остается прежним. Вопросами первостепенной важности, вероятно, следует считать необходимость обеспечить при первой же возможности физическое завладение компьютерами или подобными устройствами, предположительно использовавшимися подозреваемыми, а также необходимость принятия надлежащих мер в соответствии с общепризнанной установившейся практикой для защиты целостности этих вещественных доказательств (то есть установление режима охраны/предъявления доказательств) и проведения любой криминалистической экспертизы цифровых

данных. Несоблюдение этих процедур потенциально может повлиять на допустимость этого вида доказательств. К другим видам доказательств, которые могут требовать соблюдения особой осторожности, относятся материалы, полученные в результате обысков и/или мероприятий по наблюдению, которые должны проводиться только согласно условиям соответствующего разрешения суда.

318. При решении вопросов доказательственной базы на этапе следствия важно, чтобы у следователей было достаточное понимание правовых норм/принципов, применимых к предпринимаемым ими в рамках расследования следственным действиям, и/или чтобы они поддерживали тесную связь с обвинителями, как предоставляя им свежие данные, так и обращаясь к ним за консультациями по правовым вопросам. В случаях, когда компетентные органы одной страны ведут сбор доказательств для использования их в ходе уголовного процесса, который будет проходить в другой стране, очень важны тесные контакты и координация с зарубежными коллегами в отношении мер, принимаемых для сбора и сохранения улик. В рамках такой координации важно, чтобы сотрудники проводящего следственные действия компетентного органа ясно представляли себе требования в отношении представления доказательств, а также последствия, которые могут повлечь за собой их действия в той юрисдикции, где эти доказательства в конечном счете будут использоваться. Вопросы допустимости собранных за рубежом доказательств по делам о терроризме в более широком плане рассматриваются в Обзоре дел о терроризме ЮНОДК[153].

5. Критерий "двойной уголовной ответственности"

319. Одно из требований, обычно содержащихся в универсальных документах о противодействии терроризму и других международных, региональных и двусторонних документах, касающихся терроризма и транснациональной организованной преступности, состоит в том, что основанием для международного сотрудничества может стать только противоправное поведение, считающееся уголовно наказуемым преступлением как в запрашивающем, так и в запрашиваемом государстве. Выполнение данного требования, известного как критерий "двойной уголовной ответственности", может создавать трудности при любых связанных с какими-либо элементами международного сотрудничества уголовных расследованиях и судебных процессах, а не только в рамках дел, которые касаются борьбы с терроризмом. Несколько участников совещания группы экспертов охарактеризовали критерий "двойной уголовной ответственности" как нерешенную глубинную проблему, которая нередко ведет к отказам в удовлетворении запросов о взаимной правовой помощи или выдаче, если органы власти запрашиваемых стран полагают, что требования в отношении "двойной уголовной ответственности" не были выполнены.

320. В контексте борьбы с терроризмом в отсутствие каких-либо возлагаемых на государства универсальных обязательств в отношении криминализации конкретных видов противоправного поведения, которые реализуются через Интернет, центральным органам власти при направлении или получении запросов о международном сотрудничестве скорее всего придется ориентироваться на составы уголовных преступлений, признаваемых таковыми в касающемся терроризма законодательстве или в национальных уголовных кодексах. Например, в случае предполагаемых актов подстрекательства к терроризму, совершаемых с использованием Интернета, из-за различий в правовых подходах, которым государства следуют в отношении такого поведения, запросы о международном сотрудничестве, возможно, необходимо будет обосновывать ссылками на такие усеченные составы преступлений, как подстрекательство к совершению преступления.

[153] См.: Управление Организации Объединенных Наций по наркотикам и преступности, Обзор дел о терроризме, пункты 292–295.

321. При решении этого вопроса желательно, чтобы правительства, криминализуя связанные с терроризмом противоправные действия, в связи с которыми имеется запрос, использовали формулировки составов преступлений, максимально приближенные к тем, которые содержатся в соответствующих документах. Кроме того, в пределах, разрешенных в рамках национальных правовых систем, законодательство должно быть составлено таким образом, чтобы не быть чрезмерно ограничительным в вопросе о "двойной уголовной ответственности", предоставляя центральным органам власти и судьям достаточную свободу действий, чтобы можно было сосредоточиться на содержании противоправного поведения, являющегося предметом запроса, и оценивать именно его, а не следовать излишне узкому подходу. Если такой подход к законодательству будет в равной мере принят всеми государствами, можно будет реализовать все преимущества гармонизации законодательства, идея которой заложена в универсальных документах, и снизить возможности возникновения проблем в связи с критерием "двойной уголовной ответственности".

322. Таким образом, проблемы в связи с принципом "двойной уголовной ответственности" могут в целом создавать трудности в уголовных делах, требующих международного сотрудничества, однако они могут оказаться особенно значительными в случаях, касающихся определенных видов связанных с терроризмом преступлений, которые совершаются с использованием Интернета (например, подстрекательство), когда риски несовместимости между национальными законодательными и конституционными рамками соответствующих государств могут быть выше. Один из примеров, обсуждавшихся на совещании группы экспертов, касается позиции в отношении выдачи из Соединенных Штатов лиц, обвиняемых в преступном подстрекательстве. В этой стране действуют сильные конституционные гарантии в отношении свободы слова, закрепленные в Первой поправке к Конституции Соединенных Штатов. По законам Соединенных Штатов, заявления, составляющие независимую пропаганду любых идеологических, религиозных или политических воззрений, сами по себе не считаются преступными деяниями, хотя они могут также рассматриваться как акты, равноценные распространению информации по указанию террористической организации или в целях управления действиями такой организации, или же подпадать под статью о преступном подстрекательстве. Учитывая эту позицию, удовлетворение запросов о взаимной правовой помощи или выдаче в связи с предполагаемыми актами подстрекательства, затрагивающих какой-либо конституционный элемент в Соединенных Штатах, может оказаться проблематичным с точки зрения концепции "двойной уголовной ответственности", что требует от компетентных органов обеих стран применения гибкого и прагматичного подхода.

323. Помимо наличия совместимого законодательства и гибкого подхода к применению такого законодательства, важно, чтобы следователи, обвинители и судьи были хорошо подготовлены и понимали, как механизмы международного сотрудничества вписываются в систему ответных мер международного сообщества в борьбе с терроризмом и транснациональной организованной преступностью.

6. Различия в применении конституционных гарантий и гарантий в области прав человека

324. Вопросы, связанные с правами человека и конституционными гарантиями, имеют отношение ко многим проблемам в рамках расследования и уголовного преследования террористической деятельности, в том числе связанным с международным сотрудничеством. С другой стороны, на примере актов, относящихся к подстрекательству к терроризму, видно, что различные национальные подходы к осуществлению конституционных прав и/или прав человека могут находить отражение в различных подходах к правовым вопросам. Это может вести к возникновению трудностей в международном сотрудничестве по делам, в связи с которыми государства пытаются запросить или оказать помощь. Например, когда сотрудники компетентных органов одной страны обращаются к своим коллегам в другой стране с просьбой

предоставить связанные с Интернетом данные в отношении сделанных через Интернет заявлений, которые составляют подстрекательство к совершению террористических актов в их юрисдикции, весьма актуальным будет вопрос о том, считаются ли предполагаемые действия преступлением также и в запрашиваемой стране. В более широком контексте установления контроля за контентом Интернета, когда органы власти в одной стране добиваются удаления контента, который они рассматривают как подстрекательство к терроризму и который размещен на сервере, находящемся в другой юрисдикции, они могут столкнуться с различиями в применимых законах и конституционных гарантиях прав, таких как право на свободу выражения мнений.

325. Это особенно касается ситуации, связанной с некоторыми видами относящегося к терроризму контента электронной почты или Интернета, отправляемого через базирующихся в Соединенных Штатах провайдеров услуг Интернет или хранящегося у них. В зависимости от характера и текущего статуса такого контента, в связи с этими делами, подпадающими под юрисдикцию Соединенных Штатов, могут возникать проблемы, учитывая твердые гарантии свободы слова, предоставляемые Первой поправкой к Конституции Соединенных Штатов. В таких случаях компетентным органам в разных странах нужно поддерживать тесные контакты друг с другом, чтобы определить, какие действия, например в виде профилактических мер или уголовного преследования, которые отвечали бы их соответствующим национальным законам, правовым и культурным нормам и международным обязательствам в отношении борьбы с терроризмом, могут быть предприняты и могут ли они быть предприняты вообще.

7. Совпадающая юрисдикция

326. В связи с делами о терроризме, в которых составные элементы преступлений осуществляются с использованием Интернета, могут возникать сложные вопросы юрисдикции, особенно когда подозреваемый правонарушитель находится в одной стране и использует для совершения составных элементов преступления интернет-сайты или службы, предоставляемые провайдерами услуг Интернет в другой. Известны случаи, когда лица, постоянно проживавшие в одной стране, создавали, администрировали и обслуживали веб-сайты, которые использовались для пропаганды джихада и других связанных с терроризмом целей в других странах.

327. Одним из примеров этого является рассматривавшееся в Бельгии дело *Малика эль-Аруд и другие* (см. пункт 377). Обвиняемая, проживавшая в Бельгии, являлась администратором размещенного в Канаде веб-сайта, который она использовала для пропаганды джихада и других целей по поддержке террористической деятельности. Уголовное преследование за террористическую деятельность в таких ситуациях в значительной степени зависит от эффективного международного сотрудничества.

328. В международном праве не существует никаких обязательных норм в отношении того, как государствам надлежит вести себя в ситуациях, когда более чем одно государство может установить юрисдикцию в отношении уголовного преследования за преступление, совершенное одним и тем же подозреваемым. Хотя государства обладают широкой свободой выбора применяемых критериев, как правило, это предполагает уравновешивание или взвешивание различных факторов. В их число могут входить факторы, определяющие относительную "возможность установления взаимосвязи" между предполагаемым преступлением и конкретными государствами, включая гражданство подозреваемого, место совершения различных деяний, в целом образующих преступление, местонахождение соответствующих свидетелей и доказательств, а также относительные потенциальные трудности сбора, передачи или представления доказательств в конкретной юрисдикции. В ряде государств, включая Бельгию, Испанию и Канаду, некоторые формы юрисдикции считаются вспомогательными по отношению к другим. Считается, что первичной юрисдикцией обладают государства, наиболее тесно связанные с преступлением (например, если преступление совершено на их территории или

одним из их граждан), тогда как государства, обладающие юрисдикцией по иным основаниям, вступают в дело только тогда, когда государство, обладающее первичной юрисдикцией, не хочет или не может осуществлять судебное преследование[154].

329. В отдельных странах, включая Канаду, при установлении наличия уголовной юрисдикции применяется критерий "реальной и существенной связи"[155]. В Израиле при поступлении запросов о международном сотрудничестве от других стран по ним проводится расследование внутри страны, чтобы установить, не может ли быть доказан факт совершения преступления по израильским законам, в связи с которым судебное преследование должно быть осуществлено в Израиле. Если результатом такого расследования не становится возбуждение уголовного дела, израильские органы власти по официальным каналам передают все имеющиеся доказательства [и переводят подозреваемого в совершении преступления] в запрашивающую страну в целях осуществления там уголовного преследования. В Соединенном Королевстве законодательство и прецедентное право в отношении определенных преступлений, связанных с терроризмом, когда речь идет о деятельности за пределами Соединенного Королевства (в том числе с использованием Интернета), позволяет британским органам власти притязать на наличие юрисдикции, если можно показать, что деятельность, составляющая преступление, "в значительной мере" осуществлялась в Соединенном Королевстве, и если можно обоснованно утверждать, что эта деятельность не должна рассматриваться в суде другой страны.

330. При решении вопросов, касающихся совпадающей юрисдикции или связанного с этим международного сотрудничества, представители центральных органов власти (чаще обвинители) должны уже на раннем этапе быть осведомлены о необходимости скорейшего установления в духе сотрудничества связей со своими коллегами в других юрисдикциях, которые могут быть заинтересованы в возбуждении дела против того же подозреваемого правонарушителя. Решение о том, когда и как инициировать установление таких связей, должно приниматься на разовой основе после всестороннего рассмотрения различных факторов, которые могут действовать в данном конкретном случае. Полезные рекомендации для представителей обвинения, занимающихся рассмотрением таких вопросов, можно найти в изданном в 2007 году генеральным прокурором Соединенного Королевства и министром юстиции Соединенных Штатов Руководстве по рассмотрению уголовных дел в случаях совпадения юрисдикции Соединенного Королевства и Соединенных Штатов[156], которым предусматривается повышение эффективности обмена информацией и контактов между обвинителями в двух странах в контексте "наиболее серьезных, деликатных или сложных уголовных дел" (о которых идет речь в этом докладе). В качестве критерия для инициирования таких контактов в докладе предусматривается следующее: "Создается ли впечатление, что существует реальная возможность того, что обвинители в [другой стране] могут быть заинтересованы в возбуждении уголовного преследования по данному делу? Такое дело, как правило, должно быть в значительной мере связано с [другой страной]". В то время как сроки и способы установления контактов по вопросам юрисдикции и международного сотрудничества неизбежно будут меняться в зависимости от обстоятельств конкретного дела, обвинители, возможно, сочтут этот критерий полезной рекомендацией для применения в процессе своей работы.

[154] International Bar Association, Legal Practice Division, *Report of the Task Force on Extraterritorial Jurisdiction* (2008), pp. 172-173.

[155] *R. v. Hape* [2007] 2 SCR.292, 2007 SCC 26, para. 62.

[156] См. по адресу: www.publications.parliament.uk/pa/ld200607/ldlwa/70125ws1.pdf.

8. Национальные законы о неприкосновенности частной жизни и о защите информации

331. Национальное законодательство о защите информации и неприкосновенности частной жизни граждан нередко может ограничивать возможности правоохранительных органов и разведывательных служб делиться сведениями с партнерами как внутри страны, так и за рубежом. Здесь вновь установление надлежащего баланса между правом человека на неприкосновенность частной жизни и законной заинтересованностью государства в эффективном расследовании преступлений и уголовном преследовании за их совершение остается актуальной задачей для правительств и в некоторых случаях (в том числе в случае борьбы с терроризмом) становится предметом обеспокоенности[157].

332. В дополнение к законодательству, которое служит четким руководством для следователей, обвинителей и (когда речь идет об интернет-данных) провайдеров услуг Интернет, у которых хранятся такие данные, в отношении обязательств по сбору и использованию персональных данных, не менее важно, чтобы страны создали и ввели в действие эффективные механизмы надзора за деятельностью разведывательных и правоохранительных органов. Правительства должны обеспечить, чтобы их национальными законами были предусмотрены надлежащие механизмы, позволяющие компетентным органам, на условиях соблюдения соответствующих гарантий неприкосновенности частной жизни, делиться информацией, относящейся к расследованию и уголовному преследованию по делам о терроризме, с коллегами как на национальном, так и на международном уровне.

9. Запросы на основании договора в отличие от запросов, не основанных на договоре

333. Национальные подходы в отношении содействия выполнению не основанных на договоре запросов о сотрудничестве могут различаться, поскольку в ряде стран возможности участия в официальном сотрудничестве в отсутствие договора ограниченны. С учетом этого обстоятельства в универсальных документах по борьбе с терроризмом и транснациональной организованной преступностью содержатся положения, предусматривающие, что в качестве правового основания для сотрудничества должны рассматриваться сами эти документы, а также указывающие, какие виды противоправных деяний должны считаться преступлениями, могущими служить основанием для оказания взаимной правовой помощи и выдачи в рамках национального права государств-участников.

334. Многие страны, включая Китай, в качестве основы для участия в международном сотрудничестве опираются на принцип взаимности. По законам Китая правоохранительные и судебные органы могут участвовать в международном сотрудничестве, включая оказание взаимной помощи и сотрудничество судебных органов (включая выдачу), на договорной основе. В отсутствие договора правовой основой для сотрудничества в виде взаимной помощи и выдачи может также служить принцип взаимности. На совещании группы экспертов специалист из Китая привел пример успешного сотрудничества между компетентными органами Китая и Соединенных Штатов, результатом которого стало закрытие крупнейшего в мире порнографического веб-сайта на китайском языке, организованного в Соединенных Штатах и ориентированного на пользователей Интернета в Китае и других азиатских странах.

[157] См. Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом за 2009 год (A/HRC/10/3), в котором Специальный докладчик выразил обеспокоенность в связи с нарушением прав личности на неприкосновенность частной жизни, порождаемым усилением слежки и расширением обменов разведывательной информацией между государственными ведомствами.

335. Ряд участников совещания группы экспертов упоминали о спорных вопросах, возникающих в связи с деликатным характером значительной части информации (нередко основанной на разведывательных данных), относящейся к расследованиям по делам о терроризме, и о проблемах, с которыми неизбежно сталкиваются, не только в контексте международного сотрудничества, но и на национальном уровне, учреждения, желающие поделиться такой информацией с коллегами. Некоторые эксперты подчеркивали, что зачастую информация носит чрезвычайно секретный характер и что совместное использование ее становится затруднительным ввиду отсутствия официального механизма обмена информацией, которым предусматривались бы надлежащие условия в отношении ее использования и раскрытия.

336. В следующей главе о судебном преследовании данный вопрос рассматривается более подробно в контексте проблем доказывания, связанных с преобразованием материалов разведки в допустимые доказательства и предъявлением доказательств в процессе уголовного судопроизводства.

VI. Судебное преследование

A. Введение

337. Неотъемлемой частью универсального правового механизма по борьбе с терроризмом, а также Глобальной контртеррористической стратегии Организации Объединенных Наций является налагаемое на государства обязательство отказывать в убежище лицам, совершающим террористические акты, и привлекать их к судебной ответственности, где бы такие акты ни были совершены. Для достижения последней из этих целей странам необходимо не только эффективное законодательство о борьбе с терроризмом, криминализующее совершение террористических актов и содействующее необходимому международному сотрудничеству, но и способность применять специальные методы расследования и стратегии судебного преследования, чтобы обеспечить сбор, сохранение, представление и допустимость доказательств (нередко основанных на данных разведки) при привлечении подозреваемых в терроризме к суду, гарантируя при этом соблюдение международных норм обращения с обвиняемыми.

338. Роль обвинителей в уголовном преследовании по делам о терроризме становится все более сложной и ответственной. В дополнение к ответственности за ведение уголовного преследования обвинители в делах о терроризме становятся все более активными участниками этапов следствия и сбора разведывательной информации, обеспечивая руководство или надзор в вопросах, касающихся правовых и стратегических последствий различных методов ведения расследования. В настоящей главе рассматривается роль обвинителей в делах о терроризме, связанных с использованием террористами Интернета, в целях выявления, с точки зрения стороны обвинения, общих проблем или препятствий, а также стратегий и подходов, подтвердивших свою эффективность в процессе успешного уголовного преследования виновных в терроризме.

B. Подход к уголовному преследованию с позиций верховенства права

339. Расследование и судебное преследование, которые не проводятся в полном соответствии с принципами, обычно связываемыми с верховенством права и международными стандартами в области защиты прав человека, ставят под угрозу целостность самой ткани социальных и институциональных норм и структур, которые террористы стремятся подорвать. Поэтому принципиально важно, чтобы любое судебное преследование лиц, виновных в совершении террористических актов, осуществлялось с максимальным вниманием к необходимости обеспечения справедливого судебного разбирательства и справедливого обращения с обвиняемыми.

340. Общепризнанный принцип, согласно которому подозреваемым в терроризме должны предоставляться те же процессуальные гарантии в рамках уголовного права, что и любым другим подозреваемым преступникам, прочно закреплен и отражен в универсальных документах по борьбе с терроризмом и на политическом уровне в международном масштабе. Лишь одним из множества примеров признания этого принципа на высоком уровне является резолюция 59/195 Генеральной Ассамблеи о правах человека и терроризме, в которой Ассамблея подчеркнула необходимость усиления эффективного международного сотрудничества в борьбе с терроризмом в соответствии с международным правом, включая нормы международного права в области прав человека и международного гуманитарного права. Помимо включения этого основополагающего принципа на политическом уровне, Организация Объединенных Наций, через своего Специального докладчика по вопросу о поощрении и защите

прав человека и основных свобод в условиях борьбы с терроризмом, регулярно представляет Совету по правам человека и Генеральной Ассамблее доклады по проблемным областям, которые связаны с затрагивающими права человека аспектами мер в области уголовного правосудия, направленных на борьбу с терроризмом, и готовит рекомендации относительно принятия соответствующими сторонами мер по исправлению ситуации. В число поднятых Специальным докладчиком проблем входят вопросы, связанные с заключением подозреваемых под стражу и предъявлением им обвинений[158].

341. Известен ряд публикаций, специально посвященных вопросам поощрения прав человека и верховенства права в сфере деятельности обвинителей и сотрудников системы уголовного правосудия, причастных к осуществлению судебного преследования террористов. В 2003 году Управление Верховного комиссара Организации Объединенных Наций по правам человека подготовило Сборник по практике Организации Объединенных Наций и региональных организаций в области защиты прав человека в условиях борьбы с терроризмом. В рамках Совета Европы, который полностью признает обязательство осуществлять защиту прав человека и включает его в качестве одного из основополагающих принципов в свои документы по предупреждению преступности и вопросам уголовного правосудия, включая терроризм, данный принцип подтвержден в Руководящих принципах Комитета министров Совета Европы в области прав человека и борьбы с терроризмом, утвержденных Комитетом министров 11 июля 2002 года[159]. В этих документах содержатся ценные рекомендации для обвинителей, работающих в области борьбы с терроризмом.

C. Роль обвинителей в делах, связанных с терроризмом

342. Роль обвинителя в осуществлении уголовного судопроизводства, в том числе по делам о терроризме, различается по странам. В ряде стран, особенно в юрисдикциях континентального права, на обвинителей официально возлагаются функции по надзору за проведением уголовных расследований, руководству следственными группами на всем протяжении следствия, принятию решений относительно мероприятий по проведению обысков и наблюдения, предъявлению обвинений или подготовке обвинительных актов, решению вопросов международного сотрудничества и ведению судебных заседаний в судах.

343. В разыскных судебных системах, таких как французская, например, на обвинителя, как правило, возлагаются задачи по возбуждению дел в суде, началу предварительных расследований, определению составов преступлений; однако официальное судебное расследование, сбор и исследование доказательств ведет следственный судья или судебный следователь (juge d'instruction). Если виновность обвиняемого может быть исключена, следственный судья закрывает дело; в противном случае дело обвиняемого передается на рассмотрение другому судье. В делах о терроризме, помимо представления судье версии обвинения, главный обвинитель может ходатайствовать или внести предложение о проведении дальнейшего расследования.

344. В других странах, особенно в юрисдикциях общего права, обвинители традиционно не столь непосредственно вовлечены в проведение уголовных расследований и не несут за этот процесс такой ответственности; руководство проведением уголовных расследований обычно осуществляют правоохранительные органы. Как правило, в этих юрисдикциях обвинители берут на себя официальную ответственность за ведение судебного преследования с момента

[158] Там же.

[159] Любой созданный в рамках Совета Европы текст, независимо от того, идет ли речь об имеющих обязательную силу конвенциях или о документах из разряда "мягкого права", таких как рекомендации или резолюции, издаваемые Парламентской ассамблеей или Комитетом министров, включая любые руководства по различным вопросам, всегда должен находиться в соответствии с обширной судебной практикой Европейского суда по правам человека по соответствующему вопросу.

предъявления обвинения или вынесения обвинительного акта и до окончательного разрешения дела. Например, в Нигерии ответственность за проведение уголовных расследований несет национальная полиция. По завершении дела передаются в органы уголовного преследования, которые отвечают за предъявление обвинения и проведение уголовного судопроизводства.

345. Сходного подхода также придерживаются в Индонезии, где существует разделение между расследованием и судебным преследованием по уголовному делу. После начала расследования по уголовному делу следователь обязан отчитываться о ходе дела перед государственным обвинителем (пункт 1 статьи 109 Уголовно-процессуального кодекса Индонезии), а по завершении расследования досье по делу должно быть передано государственному обвинителю (пункт 1 статьи 110 Уголовно-процессуального кодекса), которому предстоит решить, можно ли передавать это дело в суд (статья 139 Уголовно-процессуального кодекса).

346. Однако вне зависимости от специфики конкретных юрисдикций роль обвинителей в делах о терроризме продолжает расширяться в связи с возрастающими требованиями, предъявляемыми к ним из-за непрекращающегося изменения видов, методов совершения и сложности связанных с терроризмом преступлений, законов о борьбе с терроризмом, появления новых следственных методик и механизмов международного сотрудничества.

347. Как показывает опыт, от обвинителей все чаще требуется играть более непосредственную роль в расследовании преступлений, а не только на этапе судебного преследования. Обвинители все в большей мере берут на себя выполнение функций более технического и стратегического характера, не только донося информацию о политике и законодательстве в области борьбы с терроризмом, но также предоставляя в ходе расследований юридические и стратегические консультации и рекомендации по правовым вопросам, которые влияют на вероятность успеха любого судебного преследования по результатам этих расследований. Опыт показывает, что выполнение этих функций может осуществляться в рамках междисциплинарных групп из представителей нескольких юрисдикций[160].

348. Кроме того, по мере роста прозрачности судебного преследования террористов и повышения внимания к нему, включая освещение в средствах массовой информации и мониторинг со стороны правозащитных групп и международных органов, на обвинителей ложится решающая роль в обеспечении того, чтобы расследования и судебное преследование не только велись справедливо, эффективно и с соблюдением международных стандартов в области защиты прав человека, но и чтобы это было видно широкой общественности.

D. Стадия расследования

349. В процессе сбора информации или на следственном этапе операций по борьбе с терроризмом обвинителям нередко приходится консультировать по вопросам, связанным с применением особых следственных методик.

1. Особые следственные методики

350. В то время как новые или развивающиеся технологии и методики проведения обысков и наблюдения обеспечивают разведывательным службам и правоохранительным органам более широкие возможности для отслеживания деятельности террористов в Интернете, они также несут с собой правовые риски в плане осуществления судебного преследования,

[160] Ивон Дандюран. "Роль обвинителей в поощрении и укреплении верховенства права" – документ, представленный на втором Всемирном саммите генеральных атторнеев и генеральных прокуроров, главных обвинителей и министров юстиции, состоявшемся в Дохе 14–16 ноября 2005 года.

в отношении которых обвинителям надлежит постоянно сохранять бдительность. Кроме того, ввиду различий в национальных законах, касающихся сбора и допустимости доказательств, эти риски оказываются значительнее, когда действия, направленные на получение доказательств, происходят не в той юрисдикции, в которой будет вестись судебное преследование. На европейском уровне Совет Европы, осознавая эти риски и вытекающие из обстоятельств проблемы в области прав человека, разработал рекомендации по применению особых следственных методик в связи с серьезными преступлениями, включая террористические акты[161], в которой содержатся, в частности, общие принципы, руководящие принципы оперативного характера и глава о международном сотрудничестве.

351. Связанные с вновь возникающими следственными методиками правовые риски подтверждают необходимость активного привлечения обвинителей, на возможно более ранней стадии, к принятию решений, выносимых в ходе следственного этапа дел о терроризме, чтобы гарантировать, что принимаемые при сборе потенциальных доказательств меры не поставят под угрозу успех любого последующего судебного преследования. Вопросы, касающиеся допустимости доказательств, более подробно рассматриваются в другой части настоящей главы.

352. Постоянные и быстрые изменения технологических возможностей разведывательных и правоохранительных органов по ведению наблюдения и мониторинга, а также сбору разведывательных данных или доказательств террористической деятельности подчеркивают исключительную важность функции обвинителя по консультированию следователей о правовых последствиях мероприятий такого рода для осуществления судебного преследования. Кроме того, учитывая рост вероятности того, что компетентным органам, особенно в делах о связанной с Интернетом деятельности, осуществляемой через национальные границы, потребуются координация и сотрудничество с зарубежными коллегами по соответствующим правовым вопросам (например, относительно сохранения связанных с Интернетом данных, которые находятся у провайдеров услуг Интернет), все более повышается необходимость проведения при первой же возможности консультаций с обвинителями и участия последних в принятии решений о стратегиях следствия.

2. Использование многофункциональных групп

353. Компетентные органы в своей работе по препятствованию, пресечению террористической деятельности и уголовному преследованию за нее все чаще обращаются к использованию междисциплинарных/межведомственных групп в составе представителей правоохранительных и разведывательных органов, а также обвинителей. Кроме того, между национальными правоохранительными органами, разведывательными службами и органами уголовного преследования должны существовать высокий уровень доверия, координация и линии коммуникации, что, как отмечалось на совещании группы экспертов, имеет жизненно важное значение для эффективного сотрудничества на международном уровне. Хотя пока еще не существует единого подхода, пользуясь которым можно было бы содействовать развитию данных элементов, укреплению этих важных национальных партнерств будет способствовать четкое понимание мандатов и роли участвующих ведомств, наличие надлежащих правомочий и механизмов по обмену информацией (возможно, на основе меморандумов о взаимопонимании или аналогичных договоренностей), а также регулярное проведение координационных совещаний или учебных мероприятий.

354. Несмотря на неодинаковые подходы компетентных органов разных стран к координации и проведению межведомственных расследований, в этой области имеется ряд общих черт. В Соединенных Штатах при проведении расследований в связи с совершенными в этой

[161] Комитет министров Совета Европы, Рекомендация Rec (2005)10 (от 20 апреля 2005 года).

стране террористическими актами преобладает подход, ориентированный на создание целевых групп, в рамках которого используются междисциплинарные группы из представителей всех соответствующих учреждений, включая обвинителей.

355. В соответствии с этим подходом обвинители включаются в состав групп из представителей разведывательных, правоохранительных и других специализированных органов и являются их неотъемлемой частью. Эти группы постоянно ведут мониторинг, оценку и переоценку различных аспектов расследований по подозрениям в террористической деятельности. Целевые группы по борьбе с терроризмом и/или объединенные контртеррористические целевые группы координируют усилия местных и федеральных правоохранительных органов и прокуратуры, а также их деятельность на уровне штатов. В таких целевых группах участвуют многие органы обвинения на уровне штатов и федеральном уровне, а их методы и задачи варьируются в диапазоне от участия в межведомственных совещаниях до параллельного назначения персонала, а также консультирования по различным вопросам: от получения ордеров на обыск до проведения обзоров дел и вынесения рекомендаций в отношении предъявления обвинений[162].

356. В Канаде органы власти используют объединенные группы по обеспечению национальной безопасности (INSET). По делу Намуха в состав такой группы входили представители Королевской канадской конной полиции, Канадского агентства пограничных служб, Канадской разведывательной службы по обеспечению безопасности, Полиции провинции Квебек, Полицейской службы Монреаля и прокуратуры Канадской службы государственного обвинения.

357. В Японии стало обычной практикой, чтобы при проведении связанных с терроризмом расследований полиция, хотя она является юридически независимой, информировала о соответствующих делах государственного обвинителя уже на ранних стадиях следствия и консультировалась с ним при оценке доказательств и толковании законов[163]. Аналогичного подхода также придерживаются в Египте.

358. В целях повышения эффективности и результативности направленного на борьбу с терроризмом судебного преследования правительства нередко создают в рамках национальных органов прокуратуры специализированные отделы или подразделения по делам, связанным с терроризмом. Так обстоит дело в Индонезии, где был принят ряд специальных мер, включая создание в составе Генеральной прокуратуры целевой группы по уголовному преследованию по делам о терроризме и транснациональной преступности. На эту целевую группу возлагаются обязанности по оказанию содействия и ускорению правоприменительной деятельности как на стадии расследования, за счет координации действий с полицией (например, путем участия государственных обвинителей в ходе допросов подозреваемых), так и на любых последующих этапах судебного преследования вплоть до окончательного исполнения решения суда.

359. Хотя на международном уровне способы привлечения обвинителей к участию в уголовных расследованиях и их включения в такую деятельность могут различаться, принятый во многих странах общий подход свидетельствует о желательности такого их включения и следования междисциплинарному комплексному подходу к принятию стратегических и оперативных решений на этапе расследования дел о терроризме.

[162] M. Elaine Nugent and others, *Local Prosecutors' Response to Terrorism* (Alexandria, Virginia, American Prosecutors Research Institute, 2005).

[163] Управление Организации Объединенных Наций по наркотикам и преступности, Обзор дел о терроризме, пункт 212.

E. Международное сотрудничество

360. Вопросы, касающиеся международного сотрудничества, уже были рассмотрены в главе V, выше, и возвращаться к ним здесь нет необходимости. Поднятые на совещании группы экспертов конкретные вопросы, имеющие отношение к обвинителям в рамках дел с какими-либо элементами международного сотрудничества, касаются посредничества и разрешения вопросов в отношении видов сотрудничества, проблем юрисдикции, критериев "двойной уголовной ответственности" и допустимости собранных за рубежом доказательств, которые, как показывает опыт, представляют собой постоянную проблему. Учитывая общую заинтересованность всех государств в успешном уголовном преследовании за преступления, связанные с терроризмом, важно не только наличие у государств законодательной базы для содействия такому сотрудничеству, но и использование проактивного, ориентированного на сотрудничество подхода обвинителей к решению этих вопросов.

F. Стадия предъявления обвинения

1. Принятие решений о целесообразности предъявления обвинения

361. В большинстве стран обвинителям предоставляется право на широкое усмотрение при решении вопросов о том, следует ли возбуждать уголовное дело и на основе каких обвинений. Нередко такие решения принимаются в соответствии с руководящими принципами или кодексами, призванными обеспечить справедливое, прозрачное и последовательное осуществление этих дискреционных полномочий. Например, в Соединенном Королевстве обвинители принимают такого рода решения на основании Кодекса для государственных прокуроров, в котором предусмотрен порог для предъявления обвинений с учетом обоснованности доказательств и общественного интереса. Прежде чем предъявить подозреваемому обвинение в совершении конкретного преступления, обвинители должны быть убеждены в том, что имеющиеся у них доказательства открывают "реальную перспективу вынесения обвинительного приговора"[164]. Аналогичный подход применяется в Египте.

362. В контексте борьбы с терроризмом элемент общественного интереса при оценке целесообразности предъявления обвинения, вероятно, будет весьма сильным с учетом необходимости, когда только возможно, преследовать за совершение террористических актов или связанных с ними преступлений в судебном порядке, чтобы защитить общество и не допустить повторения аналогичных преступлений. Во многих случаях вопросы обоснованности имеющихся доказательств могут стать определяющими факторами, а также могут зависеть от способности использовать основанные на данных разведки доказательства без ущерба для их источников и методов сбора или для других расследований. По этой причине в ряде случаев обвинителям может потребоваться предъявить подозреваемым обвинения, не связанные конкретно с терроризмом, для того чтобы обеспечить неприкосновенность материалов разведки.

[164] Crown Prosecution Service, "The Code for Crown Prosecutors" (London, 2010). См. по адресу: www.cps.gov.uk/publications/docs/code2010english.pdf.

2. Использование общих или специально не связанных с терроризмом составов уголовных преступлений

363. В случаях, когда компетентным органам приходится вмешиваться в целях предотвращения террористических актов, прежде чем будут получены достаточные для возбуждения судебного преследования доказательства в отношении планируемых террористических актов, вполне возможно, что в целях обеспечения правового основания для своих действий им потребуется сослаться на статью о другом уголовном преступлении. Во многих случаях, когда подозреваемые террористы в рамках своей преступной деятельности используют Интернет, компетентные органы с успехом применяли взамен составов основных преступлений, связанных с планируемым террористическим актом, такие составы уголовных преступлений, как подстрекательство, сговор, участие в террористической группе или оказание ей материальной поддержки. Особенно полезно в этом контексте наличие таких составов преступлений, как подстрекательство, сговор или участие в преступном сообществе. В некоторых случаях компетентным органам удавалось использовать и другие общеуголовные составы преступлений, такие как мошенничество или правонарушения, связанные с владением запрещенными предметами (например, фальшивыми удостоверениями личности или проездными документами, оружием) или с их использованием, что дает следователям и обвинителям возможность прервать или поставить под угрозу деятельность террористических групп, прежде чем они смогут осуществить планируемое нападение или иное деяние.

G. Стадия судебного разбирательства: проблемы в отношении доказательств

1. Проблемы с использованием доказательств, основанных на данных разведки

364. Интеграция разведывательной деятельности в системы уголовного правосудия остается существенной проблемой для компетентных органов в их борьбе с терроризмом. Как отмечалось ранее, во многих случаях используемые в делах о терроризме доказательства обвинение получает из источников, связанных с разведкой. При осуществлении судебного преследования по делам, связанным с терроризмом, общая проблема для компетентных органов всех стран состоит в том, как защитить секретные материалы, на которых основаны доказательства, базирующиеся на данных разведки, и выполнить при этом свои обязательства в отношении обеспечения справедливого судебного разбирательства и эффективной защиты обвиняемых, включая обязательство раскрыть стороне защиты все существенные элементы версии обвинения.

2. Проблемы, связанные со сбором и использованием цифровых улик

365. В делах о терроризме, связанных с использованием компьютеров, других аналогичных устройств или Интернета, важную часть версии обвинения неизбежно составляют доказательства в цифровой форме. В случаях, когда подозреваемые не присутствовали физически на месте совершения террористического акта, но тем не менее способствовали совершению этого деяния посредством неких действий в Интернете, предъявление улик, несущих их "цифровые отпечатки пальцев", может служить убедительным доказательством их соучастия и виновности.

366. Опыт показывает, что использование цифровых улик неизменно ведет к возникновению вопросов в отношении их допустимости. Поэтому исключительно важно на протяжении всего расследования и судебного преследования по делу обеспечить, чтобы используемые для их

сбора, сохранения, анализа и представления методы в полной мере соответствовали правилам представления улик или процессуальным нормам и установившейся практике.

367. Цифровые улики могут быть сложны в техническом плане и включать термины и понятия, незнакомые рассматривающим дело судье, присяжным или органу правосудия. Обвинителям необходимо в тесном сотрудничестве с экспертами и следователями обдумать, как наилучшим образом представить такие доказательства, чтобы они легко поддавались пониманию и выглядели убедительно. В этом отношении полезным может оказаться использование диаграмм и аналогичных визуальных пособий, иллюстрирующих движение данных или связей между компьютерами и пользователями.

368. В рамках своей версии дела в ходе судебных процессов, основанных на той или иной форме использования компьютера, обвинению неизбежно потребуется идентифицировать обвиняемого как лицо, пользовавшееся в конкретный момент времени компьютером, устройством или услугой Интернета, использовавшихся при совершении преступления, в котором его или ее обвиняют, и доказать существование связей, подтверждающих этот факт. Это можно сделать несколькими способами: *a)* ответчик может сделать признание или признать данный факт; *b)* его или ее присутствие за компьютером может быть установлено косвенным образом (например, он или она были единственными людьми, присутствовавшими там, где находился компьютер, или на тот момент он или она являлись зарегистрированными пользователями соответствующего аппаратного или программного обеспечения либо на компьютере имеется другая информация, знать о которой может только обвиняемый); или *c)* связь может быть установлена на основе анализа содержимого устройства/услуги ответчика, которыми, как предполагается, он или она пользовались. В этом контексте обвинителю может потребоваться представить доказательство, связанное с конкретными характеристиками хранящихся на устройстве материалов (например, документа) или каких-либо замечаний, содержащихся в перехваченном сообщении, которые присущи только обвиняемому. Наконец, хотя данный способ не является безошибочным, указанные в цифровых файлах время и дата могут быть убедительным методом установления связи обвиняемого с соответствующим устройством в моменты, относящиеся ко времени совершения преступления[165].

369. Хотя конкретные детали могут отличаться, общий подход, которого придерживаются суды во многих странах при определении допустимости доказательств в уголовном судопроизводстве, основан на относимости к делу и надежности: является ли доказательство, которое желает привести та или иная сторона, относящимся к делу и надежно ли оно? В случаях, когда цифровая улика имеет отношение к делу, проблема для обвинителей в основном будет состоять в том, чтобы убедить суд в надежности этого доказательства как в плане содержания, так и методов, использованных для его получения и предъявления суду. Процесс убеждения суда в том, что доказательство в цифровом виде может быть допущено, нередко включает доказывание законности способов его получения и сохранения его целостности с момента, когда оно было получено, и до его представления в суде. Это известно как "цепочка ответственного хранения" или "цепочка представления доказательств": процедуры, как оперативные, так и правовые, в целях сохранения целостности доказательств. В большинстве стран в отношении "цепочки ответственного хранения" существуют строгие правовые нормы, которые требуют, чтобы доказательство было незамедлительно занесено в протокол, отправлено в центр, опечатано и защищено от порчи в ожидании судебного разбирательства, а в отдельных случаях сдано под надзор судебного должностного лица.

[165] United States Department of Justice, Office of Justice Programs, National Institute of Justice, *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (2007), chap. 4, sect. IV. См. по адресу: www.ncjrs.gov/pdffiles1/nij/211314.pdf.

370. В делах о терроризме, связанных со сбором и использованием перехваченных сообщений или судебных цифровых улик, обвинитель, в тесном сотрудничестве с разведывательными и/или правоохранительными органами, обязан обеспечить, чтобы такие доказательства были получены в законном порядке, а также были сохранены и представлены с соблюдением требований в отношении представления доказательств, действующих в юрисдикции, в которой они в конечном счете будут использоваться. Сбор и представление цифровых данных в качестве допустимого доказательства, особенно если они хранятся на удаленном носителе подозреваемым или связанными с ним третьими лицами в других юрисдикциях, являются сложными задачами как для следователей, так и для обвинителей. Помимо технических сложностей, связанных с захватом и сохранением целостности требуемых данных, необходимость в некоторых ситуациях полагаться на содействие иностранных органов разведки, охраны правопорядка или судебного преследования, действующих на основании иных законов и процедур, регулирующих сбор и использование таких данных, может сделать такие процессы длительными и ресурсоемкими.

371. В случае расследований, связанных со сбором цифровых данных, находящихся полностью в пределах одной юрисдикции, вопросы их допустимости в качестве доказательства скорее всего будут в значительной степени сконцентрированы вокруг правовых оснований, на которых производились их сбор, а также последующая обработка и сохранение (то есть цепочки ответственного хранения или представления доказательств). Как и всегда, необходимо позаботиться о том, чтобы правовые основы для их сбора, криминалистической экспертизы, сохранения и представления гарантированно находились в полном соответствии с действующими правилами и процедурами, касающимися допустимости доказательств.

372. В случае сбора цифровых данных в одной или более юрисдикциях в целях использования в уголовном процессе, проводимом в другой юрисдикции, ситуация оказывается значительно сложнее и требует особого внимания со стороны следователей и обвинителей.

373. После установления стороны, владеющей данными, которые имеют отношение к расследованию, а также местонахождения этих данных в зарубежной юрисдикции следователям и обвинителям надлежит как можно скорее изучить неофициальные и официальные способы их получения и сохранения в доказательственных целях. Во всех случаях, когда это возможно и осуществимо, предпочтение следует отдавать неофициальным каналам получения данных для их последующего использования в качестве доказательств при том условии, что методы, с помощью которых осуществляются их сбор, сохранение и передача в принимающую страну, отвечают действующим правилам и процедурам представления доказательств. В целях получения таких данных следователям, возможно, потребуется подумать о возможности обращения к зарубежным коллегам с соответствующей просьбой о получении ордера на обыск, чтобы произвести обыск и изъятие данных, или же, может быть, изучить возможность использования других средств (например, общедоступных веб-страниц) или обращения к добровольным иностранным свидетелям.

374. Дело, рассмотрение которого было завершено в Германии в 2009 году и которое было связано с успешным судебным преследованием четырех членов Союза исламского джихада, является иллюстрацией масштабов и сложности многих расследований и судебных процессов по делам о терроризме. В расследовании по этому делу, которое длилось девять месяцев, принимали участие более 500 сотрудников полиции; оно потребовало многих часов электронного перехвата и наблюдения, а также сбора большого количества вещественных доказательств, равно как и широкого международного сотрудничества между компетентными органами Германии и их коллегами в Турции и Соединенных Штатах. Масштаб и сложность этого дела показывают, насколько значительные ресурсы могут потребоваться для проведения расследований и судебного преследования, а также подчеркивают необходимость и достоинства командного подхода.

Фриц Геловиц, Адем Ильмаз, Даниэль Шнайдер и Атилла Селек

В сентябре 2007 года, после интенсивного расследования, немецкие компетентные органы, действуя на основании секретной информации, полученной от коллег в Соединенных Штатах, арестовали четырех членов Союза исламского джихада (часто именуемого "Зауэрландской ячейкой"), находившихся на завершающей стадии подготовки серии взрывов в различных общественных местах в Германии. В число намеченных целей входили бары и ночные клубы в ряде мест в Мюнхене, Кельне, Франкфурте, Дюссельдорфе и Дортмунде, а также база военно-воздушных сил Соединенных Штатов в Рамштайне. Как думали обвиняемые, в целом ими было накоплено огромное количество взрывчатого материала (компетентные органы тайно заменили его безвредными веществами), потенциально достаточное, чтобы превзойти по силе террористические взрывы в Мадриде (2004 год) и Лондоне (2005 год).

Трое из обвиняемых – Геловиц, Шнайдер и Селек – являлись гражданами Германии; четвертый, Ильмаз, был гражданином Турции. За несколько месяцев обвиняемые приобрели из законных источников 780 кг перекиси водорода. 4 сентября 2007 года сотрудники компетентных органов арестовали обвиняемых, когда они собрались в загородном доме в районе Германии Зауэрланд и приступили к "приготовлению" путем добавления к перекиси водорода других ингредиентов в целях усиления взрывного эффекта. (Без ведома обвиняемых компетентные органы ранее уже заменили раствор перекиси водорода более слабым, безвредным раствором.)

В августе 2008 года федеральные обвинители предъявили Геловицу, Шнайдеру и Ильмазу официальные обвинения. Селек был экстрадирован из Турции в ноябре 2008 года на основании запроса о выдаче согласно Европейской конвенции о выдаче, а официальное обвинение было предъявлено ему в декабре 2008 года. Пункты обвинения включали участие в сговоре в целях совершения убийства, подготовку к проведению взрывов и членство в террористической организации.

Судебный процесс над всеми четырьмя подсудимыми был начат в апреле 2009 года и продолжался в течение трех месяцев, прежде чем подсудимые пришли к решению признать обвинения. Объем доказательств, которые обвинение намеревалось предъявить суду, был огромен и включал 521 папку с документами (достаточно, чтобы заполнить полку длиной 42 метра) и порядка 219 свидетелей. В значительной мере версия обвинения была основана на обширных материалах электронного мониторинга и наблюдения, которые велись в ходе расследования компетентными органами Германии. Электронные методы следствия включали использование прослушивания телефонных разговоров между подсудимыми и размещение подслушивающих устройств в их машинах и доме, где они встречались для изготовления взрывных устройств на основе перекиси водорода, а также перехват их электронной почты. Обвинение предполагало представить большой объем цифровых улик; однако, пока заговор существовал, были обнаружены явные признаки того, что обвиняемые принимали меры предосторожности против наблюдения или прослушивания. В ходе длившегося девять месяцев расследования компетентные органы столкнулись с рядом технических проблем. Например, подсудимые поддерживали связь с помощью черновиков электронной почты (то есть открытия и чтения черновиков сообщений в учетных записях абонентов электронной почты), чтобы избежать перехвата правоохранительными органами, а также пользовались незащищенными беспроводными сетевыми соединениями ни в чем не повинных граждан и зашифрованной связью через провайдеров услуг интернет-телефонии (например, Skype).

Что касается Геловица, предполагаемого главаря группы, то он пользовался доступом в Интернет через незащищенные домашние беспроводные сети случайных частных лиц, использовал по меньшей мере 14 различных учетных записей электронной почты, менял номерные знаки на автомобиле и использовал полицейский сканер для мониторинга радиообменов полиции. Он защитил данные на своем компьютере с помощью шифра, который эксперты-криминалисты безуспешно пытались взломать и получить к ним доступ. Геловиц в конце концов передал им ключ шифрования, но следователи обнаружили лишь следы стертой информации.

В ходе судебного разбирательства защита оспаривала законность действий обвинения, ставя под вопрос основание для проведения расследования, которое, по утверждению защиты, было изначально недействительным, поскольку зиждилось на разведывательной информации из Соединенных Штатов, которая, как утверждала защита, включала данные электронного мониторинга обменов сообщениями между подсудимыми, что было незаконным, и была предоставлена в нарушение их прав согласно Конституции Германии.

4 марта 2010 года четверо подсудимых были признаны виновными по всем пунктам обвинения и приговорены: Геловиц и Шнайдер к 12 годам тюремного заключения, Ильмаз к 11 годам тюремного заключения и Селек к 5 годам тюремного заключения.

3. Проблемы в связи с использованием доказательств зарубежного происхождения

375. Правовые принципы и процедуры, связанные со сбором и допустимостью доказательств в уголовном судопроизводстве, нередко различаются в разных юрисдикциях. Одной из основных проблем, встающих перед следователями и обвинителями в ходе любого расследования и судебного преследования по уголовному делу с трансграничным элементом (как в запрашиваемой, так и в запрашивающей стране), является обеспечение того, чтобы необходимые доказательства были собраны, сохранены, переданы и представлены в соответствии с применяемыми в соответствующей юрисдикции правовыми процедурами и правилами доказывания и в форме, которая будет допустимой там, где состоится суд.

376. Процесс "согласования" между странами различных аспектов, касающихся средств доказывания, может быть сложным и отнимающим много времени, но он является одним из решающих факторов, определяющих успех судебного преследования. Любые юридические недостатки методов, с помощью которых производится сбор и представление доказательств, в конечном счете используемых в суде, почти наверняка будут оспорены стороной защиты.

377. Полезным примером, дающим представление о видах проблем, которые могут возникнуть в связи с этим, может служить рассматривавшееся в Бельгии дело *Малика эль-Аруд и другие*, которое было связано с деятельностью группы обвиняемых, участвовавших в создании и администрировании ряда веб-сайтов, использовавшихся для распространения террористической пропаганды и полезной для террористов информации, а также в качестве форума для общения. Некоторые из подсудимых проживали в Бельгии, однако основной веб-сайт, на котором они осуществляли свою деятельность (minbar-sos.com), был размещен в Канаде.

Малика эль-Аруд и другие

Введение

В декабре 2008 года, после длительного, интенсивного и комплексного расследования, согласованно проведенного органами разведки, охраны правопорядка и судебного преследования Франции, Бельгии, Швейцарии, Италии, Турции, Соединенных Штатов и Канады, во Франции и Бельгии по подозрению в связях с террористической организацией "Аль-Каида" был арестован ряд лиц, которым были предъявлены различные уголовные обвинения, в том числе в участии в качестве членов в террористической группе, финансировании терроризма и предоставлении террористической группе информации и материальных средств.

При совершении предполагаемых актов, которые составляют основу для этих обвинений, подозреваемые широко использовали Интернет. Расследование их деятельности включало комплексное электронное наблюдение, прослушивание телефонных разговоров и другие формы мониторинга со стороны разведывательных и правоохранительных органов. Для того чтобы довести это дело до успешного завершения, потребовалось сотрудничество компетентных органов в нескольких юрисдикциях как на официальной, так и на неофициальной основе.

Данное дело является примером в высшей степени успешного сотрудничества национальных компетентных органов всех участвовавших государств в проведении уголовного преследования по делу о терроризме, связанному с некоторыми аспектами использования Интернета, и высвечивает ряд элементов передового опыта, о которых идет речь в настоящей публикации. Упоминания об этих элементах встречаются в главах V и VI, посвященных международному сотрудничеству и судебному преследованию.

Данное дело, которое было связано с делами в ряде других стран, вращалось главным образом вокруг деятельности Малики эль-Аруд, гражданки Бельгии марокканского происхождения, и ее мужа Моеза Гарсалауи, гражданина Туниса. Они вдвоем активно участвовали в распространении радикальной джихадистской пропаганды и вербовке, организации, руководстве и финансировании группы молодых людей из Бельгии и Франции для участия в действиях джихадистов в Афганистане и других странах.

Хотя некоторые из этих видов деятельности велись другими методами, данная семейная пара широко использовала Интернет для совершения этих деяний, в том числе в целях поддержания связи. Помимо эль-Аруд и Моеза Гарсалауи (которого вместе с одним из сообщников – Хишамом Беяйо – судили заочно), в число других подсудимых входили Али эль-Ганути, Саид Арисси, Жан-Кристоф Трефуа, Абдулазиз Бастен, Мохамед эль-Амин-Бастен и Хишам Бухали Зриуль.

Рассматривавшееся в Бельгии дело тесно связано как с проведенным во Франции делом, обвиняемыми по которому проходили Валид Отмани, Хамади Азири, Самира Гамри Мелук, Хишам Беррашед и Юсеф эль-Морабит, привлеченные к судебной ответственности и осужденные Судом большой инстанции Парижа[a], так и с расследованием и уголовным преследованием в Италии по делу Бассама Аяши и Рафаэля Жандрона.

К истории вопроса

В августе 2007 года компетентные органы Бельгии получили от своих французских коллег информацию о деятельности на веб-сайте Minbar SOS (размещавшемся в Канаде), который, как они подозревали, использовался для распространения салафистской пропаганды с призывами к джихаду против Франции. В администрировании сайта подозревались эль-Аруд и Гарсалауи. В процессе следствия были выявлены и другие подобные веб-сайты.

Компетентные органы подозревали, что эль-Аруд и Гарсалауи, действуя совместно через этот сайт, занимались подбором и вербовкой лиц, проживавших в Бельгии, для участия в боевых действиях в Афганистане. Эль-Аруд размещала на сайте подстрекательские материалы, призывавшие молодых людей присоединяться к джихаду.

Малика эль-Аруд и Моез Гарсалауи

Малика эль-Аруд и Моез Гарсалауи уже были хорошо известны европейским учреждениям по борьбе с терроризмом. В 2003 году эль-Аруд привлекалась к судебной ответственности и была оправдана судом в Бельгии по подозрениям в сотрудничестве с джихадистской сетью материально-технической поддержки, которая использовалась для организации убийства одного из лидеров сопротивления талибам в сентябре 2001 года. Одним из двух нападавших был первый муж эль-Аруд.

В 2007 году против эль-Аруд и ее второго мужа Гарсалауи было возбуждено уголовное дело в Швейцарии за оказание "поддержки преступной организации" и "публичное подстрекательство к насилию и преступности" через различные веб-сайты, совместно созданные ими в Швейцарии. Эль-Аруд была осуждена и приговорена к шести месяцам лишения свободы условно Федеральным уголовным судом в Беллинцоне.

21 декабря 2007 года эль-Аруд была арестована в Бельгии по подозрению в попытке помочь заключенному Низару Т. бежать из-под стражи; однако через 24 часа ее освободили из-за недостатка доказательств. В 2004 году Низар Т. был осужден судом в Бельгии и приговорен к 10 годам тюремного заключения за подготовку нападения террористов на американскую военную базу в Кляйне-Брогель в 2007 году. Этот арест был произведен в момент, когда уже велось расследование по подозрениям в связи с ее деятельностью на сайте Minbar SOS.

Веб-сайты

Созданные эль-Аруд веб-сайты, в том числе Minbar SOS, использовались в качестве платформы для размещения пропагандистских материалов (например, видео и фотографий), распространения книг и публикаций и поддержания связей. Каждый из участников получал регистрационное имя/псевдоним и электронный адрес, чтобы они могли обмениваться приватными сообщениями, иногда зашифрованными, в закрытых дискуссионных группах, размещавшихся на этих сайтах. В них содержались инструкции, секретная информация, пропагандистские материалы и постоянные призывы к широкомасштабному джихаду. В некоторых материалах содержались явные ссылки на руководящую роль "Аль-Каиды", а также сообщения о нападениях на войска Соединенных Штатов в Ираке.

На веб-сайтах были размещены сообщения с явными угрозами (например, послание под названием "Против французского терроризма в Афганистане есть только одно средство"), а также карта парижской пригородной железнодорожной сети, на которой некоторые из основных станций были помечены символами радиоактивного или биологического загрязнения. В некоторых сообщениях содержались четкие инструкции о способах перевода средств участникам джихада. К концу 2008 года на основном сайте Minbar SOS насчитывалось более 1400 абонентов.

В рамках совместного расследования бельгийские и французские компетентные органы осуществляли перехват сообщений на веб-сайтах, электронной почты и телефонных разговоров, а также вели мониторинг и отслеживали финансовые потоки. Тем не менее, хотя бельгийские службы безопасности пристально следили за деятельностью в Интернете на сайте Minbar SOS, направленной на вербовку бойцов для отправки в Афганистан, из-за предусматриваемых бельгийским законодательством сильных гарантий свободы слова они мало что могли сделать, чтобы помешать эль-Аруд администрировать сайт.

Французский суд, в котором в конечном счете велось судебное разбирательство по данному делу в этой стране, касаясь упомянутых веб-сайтов, отметил:

> Деятельность на этих сайтах нельзя охарактеризовать просто как поиск информации или каких-то секретных сведений; напротив, она характеризуется сознательным участием в предприятии/миссии террористической направленности.

Кроме того, в своих показаниях в ходе состоявшихся позже процессов подсудимые Саид Арисси и Хишам Беяйо заявили соответственно: "Я считаю себя жертвой интернет-пропаганды" и "такие сайты, как Ribaat и Minbar SOS, оказывают влияние на людей вроде меня, которые идут воевать", что является свидетельством того воздействия, которое ведущаяся на сайте деятельность оказывает на отдельных лиц.

В одном из редких интервью для статьи, опубликованной в газете "Нью-Йорк таймс" 28 мая 2008 года, эль-Аруд назвала себя «воительницей в священной войне "Аль-Каиды"». Она настаивала, что (...) не имеет намерения самой брать в руки оружие. Она предпочитает побуждать мусульманских мужчин идти сражаться и призывает женщин присоединяться к движению. "Взрывать бомбы не мое дело – это смешно... У меня есть свое оружие. Я пишу. Я выступаю. Вот мой джихад. С помощью слов можно многое сделать. То, что я пишу, это тоже бомба"[b].

Поездка завербованных на управляемые федеральным правительством Пакистана территории племен

Помимо своей деятельности через веб-сайты, Гарсалауи также объезжал иммигрантские кварталы Брюсселя, чтобы вербовать людей лично. Арестованный по этому делу Хишам Беяйо, 23-летний гражданин Бельгии марокканского происхождения, который до своей поездки в Пакистан был администратором сайта Minbar SOS, признался, что был завербован именно таким образом.

Вербовочная деятельность Гарсалауи не ограничивалась одной Бельгией; он также завербовал двух французских пользователей сайта Minbar SOS. Один из завербованных, который выезжал на управляемые федеральным правительством Пакистана территории племен, а позже был арестован, охарактеризовал призывы к джихаду на сайте Minbar SOS как "непрестанные" и заявил, что желание стать добровольцем возникло у него под влиянием увиденных на этом сайте пропагандистских видеоматериалов.

В декабре 2007 года Гарсалауи и шестеро завербованных, в том числе Хишам Беяйо, Али эль-Ганути и Ю. Харризи, выехали на управляемые федеральным правительством Пакистана территории племен через территорию Турции и Исламской Республики Иран. Группа оставалась там до второй половины 2008 года. Находясь там, Гарсалауи постоянно поддерживал связь с эль-Аруд по электронной почте и иногда через Skype. Помимо отправки фотографий и других пропагандистских материалов, он размещал свои заявления и периодически подключался к чат-форумам на сайте Minbar SOS.

26 сентября 2008 года Гарсалауи разместил на сайте Minbar SOS заявление с призывом к осуществлению нападений в Европе: "Решение, мои братья и сестры, не фетва, а громкие взрывы", – гласило его сообщение.

Аресты

На протяжении нескольких месяцев во второй половине 2008 года некоторые из подозреваемых начали возвращаться в Бельгию. Бельгийские службы безопасности были приведены в состояние повышенной готовности, после того как из территорий племен, управляемых федеральным правительством Пакистана, вернулись эль-Ганути и Харризи, а 4 декабря 2008 года в Бельгию вернулся и сам Беяйо.

В отношении причин, по которым завербованные вернулись в Бельгию в это время, выдвигаются разные объяснения. Некоторые из подозреваемых указывали в качестве мотива на недовольство обращением с ними и условиями на управляемых федеральным правительством Пакистана территориях племен, в частности на ограниченность возможностей участия в джихаде, и отрицали существование какой-то "законсервированной ячейки", имеющей целью проведение терактов в Бельгии. Однако, по мнению бельгийских компетентных органов, данные из перехваченных сообщений давали веские основания подозревать, что эта группа, возможно, находилась на заключительной стадии планирования акции террориста-смертника (вероятно, с использованием Хишама Беяйо) на территории Бельгии, в связи с чем требовалось принять немедленные меры.

11 декабря, через неделю после возвращения Беяйо, бельгийские компетентные органы провели рейды в 16 точках Бельгии и арестовали девять подозреваемых, в том числе эль-Аруд, Гарсалауи и Беяйо. Аналогичные операции были проведены во Франции и Италии.

Уголовное преследование

Бельгия

На суде адвокаты обвиняемых оспаривали различные аспекты версии обвинения, в том числе процессуальное обоснование и допустимость некоторых доказательств, в частности полученных на неофициальной основе от ФБР связанных с Интернетом данных, касавшихся провайдеров услуг Интернет, базирующихся в Соединенных Штатах. Вопросы, касающиеся такого рода доказательств, более подробно рассматриваются далее в настоящей публикации.

Допрос Беяйо был проведен 20 мая 2008 года компетентными органами Марокко. Его адвокат утверждал, что имело место нарушение права на справедливое судебное разбирательство, основываясь на подозрениях по поводу применения марокканскими компетентными органами пыток в отношении задержанных, подозреваемых в терроризме. Суд отклонил эти доводы.

Деятельность Брайана Нила Вайнаса (Соединенные Штаты)

В январе 2009 года гражданин Соединенных Штатов Брайан Нил Вайнас отправился в Афганистан, где во время ракетного налета "Аль-Каиды" на одну из военных баз попытался убить американских солдат. Позже он был арестован и возвращен в Соединенные Штаты, где ему предъявили обвинение в сговоре в целях убийства граждан Соединенных Штатов, в оказании материальной поддержки "Аль-Каиде" и прохождении военной подготовки в рядах этой группы. Вайнас признал себя виновным и был приговорен к тюремному заключению.

Осуществляя преследование Беяйо как пособника эль-Аруд, компетентные органы Бельгии представили доказательства из судебного дела Вайнаса для определения масштаба их деятельности и факта их участия в сети "Аль-Каиды". В своих показаниях Вайнас признал, что встречался с некоторыми из завербованных в Бельгии лиц. Защита оспорила допустимость этих доказательств по ряду оснований, но ее аргументы были отклонены судом.

Исход судебного процесса

После слушания дела по существу Суд первой инстанции города Брюсселя 10 мая 2010 года исследовал вопрос о фигурировавших в делах девяти обвиняемых различных обвинениях, по которым они предстали перед судом, и разделил их на три группы: A, B и C.

К обвинениям групп A и C были отнесены соответственно участие в террористической группе в качестве одного из ее ведущих членов и участие в деятельности террористической группы, в том числе в виде предоставления информации или материальных средств или в виде финансирования деятельности террористической группы в той или иной форме, зная, что такое участие будет способствовать совершению этой группой преступления или правонарушения.

К обвинениям группы B были отнесены совершение правонарушений или оказание содействия в совершении правонарушений посредством пожертвований, обещаний, угроз, злоупотребления полномочиями или властью; участие в заговоре или сговоре с намерением совершить преступления, направленные против людей или имущества в целях нанесения серьезного ущерба; а также преступления, способные, по своему характеру или условиям совершения, нанести серьезный вред той или иной стране или международной организации, которые были умышленно совершены, с тем чтобы серьезно запугать население или противоправным путем принудить органы государственной власти или международную организацию принять те или иные меры либо серьезно дестабилизировать или разрушить основополагающие политические, конституционные, экономические или социальные основы той или иной страны или международной организации.

По обвинениям группы A были вынесены следующие приговоры:

- Малика эль-Аруд: восемь лет лишения свободы и штраф 5000 евро;
- Моез Гарсалауи: восемь лет лишения свободы и штраф 5000 евро (заочно);
- Хишам Беяйо: пять лет лишения свободы и штраф 1000 евро (заочно).

По обвинениям группы B были вынесены следующие приговоры:

- Али эль-Ганути: оправдан;
- Саид Арисси: оправдан.

По обвинениям группы C были вынесены следующие приговоры:

- Али эль-Ганути: три года лишения свободы и штраф 500 евро;
- Саид Арисси: 40 месяцев лишения свободы и штраф 500 евро;
- Хишам Бухали Зриуль: пять лет лишения свободы и штраф 2000 евро (заочно);
- Абдулазиз Бастен: 40 месяцев лишения свободы и штраф 500 евро;
- Мохамед эль-Амин-Бастен: 40 месяцев лишения свободы и штраф 500 евро;
- Жан-Кристоф Трефуа: оправдан.

Франция

Во Франции перед Судом большой инстанции города Парижа предстали пять подозреваемых (все пятеро – граждане Франции североафриканского происхождения). Валиду Отмани, Хамади Азири, Самире Гамри Мелук, Хишаму Беррашеду и Юсефу эль-Морабиту были предъявлены обвинения в совершении ряда преступлений: финансировании терроризма, заговоре в целях совершения террористического акта и участии в группе, созданной в целях подготовки террористического акта, как это предусмотрено в статье 421-1 Уголовного кодекса Франции.

Италия

Бассаму Аяши и Рафаэлю Жандрону (оба граждане Франции) компетентные органы Италии предъявили обвинение в создании преступного сообщества в террористических целях на основании пункта 1 статьи 207bis итальянского Уголовного кодекса, которым предусматривается наказание в виде лишения свободы на срок от 7 до 15 лет для лиц, признанных виновными в учреждении, пропаганде, организации, управлении или финансировании групп, предназначенных для совершения основанных на насилии актов в целях содействия достижению террористических целей или подрыва демократических устоев государства, и лишения свободы на срок от 5 до 10 лет для отдельных лиц, вступающих в такие группы.

В ходе рассмотрения дела было установлено наличие связей между двумя обвиняемыми и некоторыми из обвиняемых по бельгийскому делу, а также выявлены общие элементы улик, включая данные о DVD-диске с предсмертной запиской предполагаемого смертника, написанной одним из бельгийских подозреваемых.

3 июня 2011 года Аяши и Жандрон были приговорены к восьми годам лишения свободы.

Источник: Eurojust, *Terrorism Convictions Monitor*, Issue 8, September 2010

[a] Судебное решение от 18 февраля 2011 года (дело № 1015239014).

[b] См. "Al Qaeda warrior uses Internet to Rally Women", The New York Times (28 May 2008). См. по адресу: www.nytimes.com/2008/05/28/world/europe/28terror.html?_r=1&pagewanted=all.

378. По делу эль-Аруд сторона обвинения представила доказательства в виде интернет-данных, касающихся размещения сообщений и обсуждений в дискуссионных группах. Что касается электронных писем (последние отправлялись с учетных записей, открытых на сайтах Yahoo и Microsoft), то данные о них хранились на серверах в Соединенных Штатах. На основании неофициального запроса о помощи ФБР предоставило бельгийским компетентным органам (в двухнедельный срок) компакт-диск с данными, касающимися указанных учетных записей электронной почты и других относящихся к делу учетных записей. ФБР оговорило, что данный компакт-диск был предоставлен компаниями Yahoo и Microsoft добровольно, что допускается положениями Закона Соединенных Штатов о патриотизме.

379. Защита оспорила допустимость этих доказательств, утверждая, что примененные для сбора, передачи и представления этих доказательств процедуры были незаконными, поскольку эти доказательства были получены в отсутствие ордера на обыск, а также на том основании, что использованная неофициальная процедура не соответствует обычным методам международного обмена судебной информацией, что противоречит пункту 1 статьи 7 Закона Бельгии о международной взаимной помощи по уголовным делам от 9 декабря 2004 года.

380. Суд отклонил эту аргументацию, постановив, что: *a)* обмен информацией не происходил в рамках взаимной правовой помощи; *b)* на соответствующий момент по делу не был назначен следственный судья, и вопрос решался на неофициальной основе в рамках связей между двумя полицейскими ведомствами; и *c)* использованная процедура была оправдана ввиду чрезвычайных обстоятельств дела (то есть обнаружение размещенной одним из подозреваемых на сайте Minbar SOS предсмертной записки, дававшей основание предполагать неизбежность террористического акта на территории Франции, который готовили Малика эль-Аруд и ее сообщники). Суд признал, что по этим причинам федеральный магистрат вполне оправданно пришел к заключению, что данный чрезвычайный вариант сотрудничества между полицейскими органами был основан на положениях пункта *b)* статьи 15 Международной

конвенции о борьбе с бомбовым терроризмом (1997 год)[166], которые требуют от государств "обмена точной и проверенной информацией в соответствии со своим национальным законодательством и координации административных и других мер, принимаемых, когда это необходимо, в целях предотвращения совершения преступлений, указанных в статье 2"[167].

381. Наконец, Суд постановил, что, поскольку правовая основа для передачи информации бельгийской полиции компетентными органами Соединенных Штатов была действительной с юридической точки зрения, судебные власти Бельгии де-факто были вправе ее использовать. Суд добавил, что анализ, касавшийся зарегистрированных в Соединенных Штатах адресов электронной почты (или большинства из них), был приобщен к судебному делу после выполнения судебного поручения во Франции[168].

382. На примере данного дела видно, насколько тщательно необходимо обдумывать методы, используемые для сбора и передачи таких доказательств, уже на следственном этапе дел, в рамках которых используются доказательства из иностранных источников. Это подкрепляет подчеркивавшийся рядом специалистов на совещании группы экспертов тезис о важности того, чтобы к расследованию при первой же возможности подключались обвинители, для того чтобы еще до суда выявить и урегулировать потенциальные проблемы с доказательствами.

383. По делу *Намуха* (Канада) стороне обвинения потребовалось в ходе судебного разбирательства представить доказательства, собранные сотрудником полиции Австрии; это вызывало ряд проблем. Согласно австрийским законам свидетельство сотрудника полиции может быть допущено в качестве доказательства в виде письменных показаний. Однако не так обстоит дело согласно канадским законам, которые обычно исключают использование показаний с чужих слов и требуют, чтобы свидетели являлись в суд и давали устные показания. В целях содействия представлению показаний сотрудником полиции Австрии канадским обвинителям пришлось вступить в тесное взаимодействие с австрийской полицией и прокуратурой для разъяснения применимых правил представления доказательств согласно законодательству Канады, а также с адвокатами защиты для достижения договоренности о том, чтобы свидетельство сотрудника полиции могло быть представлено в письменной форме.

4. Использование свидетельских показаний экспертов

384. По делам, связанным с терроризмом, для того чтобы доказать тот или иной специальный аспект или аспекты дела, обвинителям нередко приходится представлять свидетельские показания экспертов. Однако круг потенциальных проблем, которые могут потребовать предъявления такого рода доказательств, весьма широк. На основе уже проведенных уголовных дел о террористической деятельности, связанной с использованием Интернета, можно в целом наметить ряд областей, в рамках которых у следователя или обвинителя может возникнуть потребность уделить внимание данному вопросу.

385. Продолжающееся быстрое развитие различных областей технологии и коммуникаций сопровождается ростом их сложности и специализации. Вполне вероятно, что обвинителям в ходе одного и того же судебного процесса может потребоваться несколько свидетелей-экспертов для объяснения различных, но взаимосвязанных технических аспектов компьютерных или коммуникационных систем или связанной с ними деятельности, особенно когда имеются доказательства того, что подозреваемый пользовался конкретным компьютером, устройством или связанной с Интернетом службой[169].

[166] United Nations, *Treaty Series*, vol. 2178, No. 38349.

[167] Eurojust, *Terrorism Conviction Monitor*, Issue 8, September 2010.

[168] Ibid.

[169] Walden, *Computer Crimes and Digital Investigations*, p. 383.

386. В случаях предполагаемого участия в террористических группах или предоставления им материальной поддержки или подстрекательства, вербовки и обучения помимо свидетельств, связанных с криминалистической экспертизой компьютеров, могут также потребоваться заключения экспертов в отношении идеологии, целей, деятельности и организационной структуры конкретных террористических групп или отдельных лиц.

387. Как правило, в случаях, связанных с использованием свидетелей-экспертов, выделяют три этапа или фазы: *a)* четкое определение проблем (и их рамок), в отношении которых требуется экспертное заключение; *b)* поиск квалифицированного специалиста; и c) обеспечение того, чтобы квалифицированный специалист использовал средства, допустимые в суде[170].

a) Четкое определение проблем

388. Действуя в тесном сотрудничестве со следователями, обвинители должны на как можно более раннем этапе определить вопросы, по которым, по их мнению, потребуются показания экспертов, и дать экспертам поручение провести необходимый анализ, предоставив четкие инструкции в отношении ключевых элементов искомых доказательств.

b) Поиск квалифицированного эксперта

389. При выборе свидетелей-экспертов для дачи экспертных показаний по специальным аспектам доказательств, фигурирующих в судебных процессах по делам о терроризме, обвинителям следует решить, использовать ли государственных или негосударственных экспертов. Хотя использование государственных экспертов допустимо и дает некоторые преимущества, это может оказаться нежелательным, если существует вероятность того, что в процессе досудебного предъявления доказательств или при перекрестном допросе таких свидетелей стороной защиты на суде могут быть раскрыты секретные источники разведывательной информации и способы получения сведений, подтверждающих их точку зрения. Для того чтобы избежать этой потенциальной ловушки, обвинителям, возможно, предпочтительнее полагаться на услуги экспертов из академических или негосударственных кругов, основывающих свои показания на общедоступной информации, которую можно раскрыть без риска поставить под угрозу источники или способы получения разведывательных сведений[171].

390. Хорошим примером использования обвинением негосударственных экспертов является дело *Намуха*, когда два свидетеля были вызваны для объяснения целей и методов деятельности Глобального исламского информационного фронта (ГИИФ). Подоплека их показаний изложена в пункте 394, ниже.

391. В менее развитых странах поиск подходящего эксперта, особенно в узкоспециальных областях, может оказаться серьезной проблемой. Обвинителям, во взаимодействии со следователями, надлежит проявить инициативу и осмотрительность, исследовав все средства, чтобы (если это возможно) на национальном уровне отыскать необходимого свидетеля, обладающего требуемой квалификацией, а в случае необходимости принять меры к поиску подходящего свидетеля на международном уровне.

c) Гарантии использования экспертом средств, допустимых в суде

392. Очевидно, что очень важно, чтобы свидетели обвинения следовали общепризнанной устоявшейся практике и применяли ее в процессе проводимой (проводимого) ими экспертизы (анализа) в конкретной области, в связи с которой их вызывают. Это особенно касается любых специальных криминалистических исследований, проводимых в целях обоснования

[170] National Institute of Justice, *Digital Evidence in the Courtroom*, chap. 3, sect. III.E.

[171] Управление Организации Объединенных Наций по наркотикам и преступности, Обзор дел о терроризме, пункт 194.

заключений, которые будут изложены в их показаниях, составляющих часть представляемых стороной обвинения доказательств. Следователям и обвинителям следует на самом раннем этапе решить, потребуются ли заключения экспертов по тем или иным специальным аспектам версии обвинения, и если да, то как можно раньше провести консультации с соответствующими специалистами и привлечь их к сотрудничеству, чтобы доказательная база последующих свидетельских показаний экспертов была гарантированно сохранена в форме, допустимой в суде.

393. В некоторых случаях, особенно связанных с компьютерными технологиями, доказательства могут носить технически сложный характер, и обвинителям и свидетелям-экспертам необходимо рассмотреть инновационные способы представления таких доказательств судьям, присяжным или другим лицам, призванным устанавливать факты в ходе судебного разбирательства, таким образом, чтобы эти доказательства были четкими, понятными и убедительными. Например, визуальное отображение построения систем или потоков данных, а не одни только устные показания, могло бы помочь лицам, призванным устанавливать факты, лучше понять технические аспекты, связанные с компьютерными или коммуникационными системами. Важно также, чтобы обвинитель обладал основательными практическими знаниями в конкретной предметной области, которые позволят ему или ей объяснять соответствующие термины и понятия судьям, присяжным или членам судейской коллегии и эффективно представлять версию обвинения.

394. В рамках рассматривавшегося в Канаде дела *Намуха* были широко использованы данные экспертизы (представленные экспертом Королевской канадской конной полиции по цифровой криминалистике) по вопросам, касавшимся цифровых улик. Последние относились в основном к предполагаемому использованию подсудимым компьютера (изъятого из его дома) и пользованию с его помощью услугами Интернета для участия в интерактивных дискуссионных форумах, загрузки материалов на веб-сайты и поддержания связи с другим сообщником, находившимся в Австрии. Эти подробные показания специалиста по вопросам цифровой криминалистической экспертизы были необходимы, чтобы убедить суд в том, что именно обвиняемый работал на компьютерах, с которых были отправлены уличающие сообщения, а также чтобы охарактеризовать идеологию и методы ГИИФ – глобальной группировки, активным участником которой являлся обвиняемый.

395. Часть защиты Намуха была направлена на подрыв этого аспекта версии обвинения. Согласно заявлениям адвокатов, в силу изначально присущей Интернету подверженности ошибкам, свидетель-эксперт не вправе ссылаться на него как на надежный источник информации для обоснования своего заключения о деятельности ГИИФ и других террористических групп. В частности, защита утверждала, что свидетели-эксперты не могли наверняка установить, на самом ли деле авторами материалов, размещенных на чат-форумах в Интернете, и других видов электронных сообщений являлись предполагаемые террористы или, напротив, их авторство может быть отнесено на счет агентов государства, действовавших в провокационных целях. В данном случае показаний, которые представил эксперт, назначенный по ходатайству обвинения, оказалось достаточно, чтобы убедить суд в надежности использованных экспертом методов и достоверности материалов из сети Интернет и придать заключению эксперта соответствующий вес.

396. Следует отметить, что обмен электронными сообщениями велся на арабском языке, затем они были переведены на французский, и сторона обвинения приобщила к судебному делу этот французский перевод вместе с оригиналом их расшифровки на арабском языке. Данный аспект дела также подчеркивает необходимость действовать с большой тщательностью, когда компетентные органы хотят представить в качестве доказательства переводы бесед или документов, включая расшифровки перехваченных сообщений на других языках.

397. Помимо экспертного заключения в отношении критически важных цифровых улик, обвинение ходатайствовало о привлечении эксперта для дачи показаний о деятельности и целях ГИИФ; его методах координации и вербовки новых членов, пропаганды радикальной идеологии и проведения военной подготовки; а также методах, используемых им для обеспечения связи через Интернет. Обвинение представило письменные отчеты двух экспертов по этим вопросам, а один из экспертов дал в суде показания, подкреплявшие изложенные в его докладе выводы. Специалист из Канады на совещании группы экспертов подчеркнул важность того, чтобы у обвинителей имелось более одного потенциального свидетеля-эксперта по ключевым элементам доказательственной базы как в целях подтверждения доказательств, так и в связи с планом чрезвычайных мер.

398. Важность такого вида свидетельских показаний экспертов в судебных процессах по обвинениям в связи с поддержкой террористических организаций иллюстрирует заявление участвовавшего в рассмотрении дела судьи в отношении "реальных действий, рекомендуемых ГИИФ", которые являлись предметом свидетельских показаний соответствующего эксперта в поддержку версии обвинения:

> Защитник подсудимого предлагает Суду рассматривать различные распространяемые ГИИФ сообщения как используемые в фигуральном смысле. У Суда нет сомнений на этот счет. Контекст этих сообщений явно указывает на то, что ГИИФ *выступает с призывами к реальным действиям*. Повсюду налицо смерть и разрушения. *Пропагандируемый ГИИФ джихад основан на насилии*. [Курсив автора.] Эта пропаганда безусловно представляет собой подстрекательство к совершению террористических актов, а иногда и угрозу их совершением. Таким образом, эта деятельность бесспорно подпадает под определение террористической деятельности по смыслу статьи 83.01 Уголовного кодекса[172].

H. Другие вопросы

1. Необходимость планирования чрезвычайных мер и обеспечения непрерывности

399. Ввиду сложности осуществления уголовного преследования по делам о терроризме, особенно если они связаны с международным сотрудничеством или с элементами высоких технологий, желательно, чтобы дела велись группами обвинителей, а каждый из членов этих групп был хорошо осведомлен о соответствующем деле и, при необходимости, достаточно компетентен, чтобы продолжить разбирательство, если кто-либо из членов группы неожиданно прекратит свое участие в деле. Данная мера предосторожности гарантирует проведение слушаний в суде на высоком уровне и сведет к минимуму вероятность неудачного исхода. Двумя полезными примерами требовавших командного подхода крупных и сложных дел, притом что по крайней мере один из обвинителей был причастен к делу на всех его этапах, являются дела Намуха (Канада) и Геловица, Ильмаза, Шнайдера и Селека (Германия). Следует отметить, что в отношении рассматривавшегося в Германии дела, по первоначальной оценке, длительность судебного процесса должна была составить два года, но фактически она оказалась намного короче, благодаря тому что подсудимые признали свою вину; однако даже при этом сам процесс занял три месяца.

[172] Justice C. Leblond, 1 October 2009.

2. Необходимость улучшения подготовки персонала и расширения его потенциала

400. В целях обеспечения комплексного подхода на основе принципа верховенства права и сохранения действенности ответных мер со стороны системы уголовного правосудия в борьбе с терроризмом страны должны непоколебимо и беспрерывно работать над расширением потенциала обвинителей в осуществлении национального законодательства по борьбе с терроризмом и связанных с этим обязательств в области международного сотрудничества. Природа контртеррористических законов и расследований, а также скорость, сложность и трансграничный характер деятельности, связанной с Интернетом, означают, что следственным группам, в том числе обвинителям, приходится в весьма сжатые сроки принимать большое количество решений по различным аспектам дела. Важно, чтобы они были надлежащим образом подготовлены и компетентны для выполнения своих основных функций в связи с делами о терроризме.

401. В странах, в которых высок риск террористической деятельности, а институциональные возможности служб уголовного преследования и других органов уголовного правосудия незначительны, первоочередное внимание следует уделять повышению потенциала специалистов этих учреждений как в плане ведения уголовных дел, так и применительно к соответствующим механизмам международного сотрудничества.

VII. Сотрудничество с частным сектором

A. Роль заинтересованных сторон из частного сектора

402. Хотя ответственность за борьбу с использованием Интернета в террористических целях в конечном счете лежит на государствах-членах, содействие основных заинтересованных сторон из частного сектора имеет решающее значение для ее эффективного осуществления. Сетевая инфраструктура интернет-сервисов нередко полностью или частично принадлежит частным организациям. Аналогичным образом, частные компании, как правило, являются владельцами социальных сетевых платформ, способствующих распространению создаваемого пользователями контента среди широкой аудитории, а также популярных поисковых систем в Интернете, осуществляющих фильтрацию контента на основе предоставляемых пользователем критериев.

403. Эффективность Интернета как среды для распространения связанного с актами терроризма контента зависит от наличия доступа к интернет-технологиям как у отправителя соответствующего сообщения, так и у его аудитории. Таким образом, основными способами ограничения воздействия сообщений такого рода являются контроль за доступом к сетевой инфраструктуре, цензурирование интернет-контента или сочетание обоих этих методов[173]. В то время как уровни государственного регулирования Интернета в разных государствах-членах существенно различаются, в отсутствие всемирного централизованного органа, ответственного за регулирование Интернета, важную роль в обеспечении контроля за доступом к распространяемому через Интернет контенту, связанному с террористической деятельностью, продолжают играть заинтересованные стороны из частного сектора, такие как провайдеры услуг, веб-сайты, предоставляющие услуги по размещению пользовательского контента, и интернет-поисковики. Саморегулирование этих принадлежащих к частному сектору заинтересованных сторон также может помочь в борьбе с проводимой с использованием Интернета деятельностью террористов по обеспечению связи, подстрекательству, радикализации и обучению боевиков. Определенную роль в своевременном выявлении деятельности в Интернете, которая может способствовать совершению террористических актов, также играют частные мониторинговые службы.

1. Провайдеры услуг Интернет

404. Во многих государствах-членах доступ пользователей к Интернету контролируется негосударственными субъектами, такими как принадлежащие к частному сектору провайдеры телекоммуникационных услуг, владеющие или управляющие сетевой инфраструктурой. Эти провайдеры услуг могут располагать широкими возможностями для оказания помощи в сборе данных о передаче сообщений или, по обстановке, для раскрытия таких данных[174], в интересах конкретного расследования потенциальной террористической деятельности, проводимого органами охраны правопорядка, уголовного правосудия и разведки. Находящиеся в распоряжении провайдеров услуг Интернет данные о передаче сообщений могут стать главными уликами против лиц, виновных в совершении преступлений, связанных с использованием Интернета, или указать путь к выявлению представляющих интерес для следствия дополнительных доказательств или соучастников.

[173] Conway, "Terrorism and Internet governance: core issues", p. 26.

[174] При условии соблюдения применимых гарантий и правил в отношении неприкосновенности частной жизни.

405. Например, провайдеры услуг Интернет могут, прежде чем открыть доступ к контенту и службам Интернета, потребовать от пользователей предоставления идентифицирующей информации. Сбор и сохранение идентифицирующей информации, связанной с пользованием данными Интернета, а также раскрытие такой информации при условии соблюдения соответствующих гарантий могут существенно помочь в проведении следствия и уголовного преследования. В частности, важным источником информации для уголовного расследования может стать требование регистрации при пользовании беспроводными сетями или интернет-кафе. В то время как в ряде стран, таких как Египет, действуют законы, требующие от провайдеров услуг идентификации личности пользователей, прежде чем предоставить им доступ в Интернет, аналогичные меры могут также приниматься провайдерами услуг Интернет на добровольной основе.

a) Сотрудничество с правительственными структурами

406. Учитывая деликатный характер дел, связанных с терроризмом, стимулом к сотрудничеству с правоохранительными органами для заинтересованных сторон в частном секторе может стать положительное воздействие такого сотрудничества на их репутацию, если оно надлежащим образом сбалансировано с должным соблюдением основных прав человека, таких как свобода выражения мнений, уважение неприкосновенности частной жизни, жилища и корреспонденции, а также право на защиту информации. Стимулирующим фактором может также служить желание избежать вытекающих из отказа от сотрудничества пагубных последствий. Например, провайдеры услуг Интернет могут сотрудничать с органами власти из опасения возможных негативных коннотаций, если их будут считать причастными к поддержке террористической деятельности. На уровень сотрудничества со стороны организаций частного сектора также может влиять боязнь ответственности в связи с размещением определенных видов интернет-контента.

407. Эксперт из Египта отметил, что национальный опыт его страны свидетельствует о готовности соответствующих заинтересованных учреждений частного сектора в духе сотрудничества откликаться на разумные просьбы государственных органов о пресечении доступа к интернет-контенту, связанному с терроризмом. Кроме того, по имеющимся сведениям, стимулом к сотрудничеству для провайдеров услуг Интернет в Египте отчасти является признание совпадения интересов этих организаций, которые сами могут становиться объектами атак террористов, и органов государственной власти, старающихся предотвращать такие террористические акты и преследовать виновных в их совершении в судебном порядке.

408. Хотя представители частного сектора могут демонстрировать готовность к добровольному удалению противозаконного контента, их также могут вынуждать к этому положения внутреннего законодательства. В Соединенном Королевстве, например, в статье 3 Закона о терроризме 2006 года предусматривается, что правоохранительные органы вправе предъявлять провайдерам услуг Интернет требования об "удалении" (см. пункт 172, выше, и далее). Требования об "удалении" используются для уведомления тех, кто предоставляет услуги по размещению контента, о том, что, согласно заключению соответствующего представителя правоохранительных органов, такой материал считается связанным с терроризмом и противозаконным. Провайдеры услуг Интернет, которым направляется требование об "удалении", обязаны удалить связанный с терроризмом контент в течение двух рабочих дней. Хотя требования об "удалении" в связи с отдельными правонарушениями также используются и в других юрисдикциях, чаще это происходит применительно к случаям нарушения авторских прав или размещения материалов откровенно сексуального содержания.

409. Государство Израиль информировало о своих успехах в сфере сотрудничества с иностранными представителями частного сектора в Израиле. Например, в ходе ряда расследований, связанных с компьютерными преступлениями, направлялись запросы представителям компаний Microsoft и Google в Израиле. По получении надлежащим образом оформленного распоряжения суда запрашиваемая следственными органами информация была предоставлена

незамедлительно. В нескольких случаях, когда возникала необходимость направить запросы представителям частного сектора, базирующимся в Соединенных Штатах, обычно использовалась официальная процедура обращения за правовой помощью по государственным каналам, однако иногда запросы о предоставлении идентификационных данных с успехом направлялись и непосредственно в адрес иностранных корпораций частного сектора.

b) Хранение данных

410. Ряд государств-членов недавно ввели или предполагают ввести в действие законодательство, требующее от провайдеров телекоммуникационных услуг на регулярной основе собирать и сохранять в архиве данные о передаче сообщений в отношении своих пользователей. В 2006 году, отчасти под влиянием террористических актов, совершенных в Мадриде в 2004 году и в Лондоне в 2005 году[175], Европейский союз принял директиву об обязательном хранении данных о коммуникационных потоках (Директива 2006/24/ЕС Европейского парламента и Совета Европейского союза от 15 марта 2006 года о хранении данных, генерируемых или обрабатываемых в связи с предоставлением общедоступных услуг электронного обмена данными или сетей связи общего пользования, изменяющая Директиву 2002/58/ЕС)[176]. В Директиве 2006/24/ЕС признается, что существование различий правового и технического характера между национальными законоположениями, касающимися подлежащих хранению видов данных, а также условий и сроков хранения таких данных, ведет к возникновению некоторых проблем[177]. Поэтому в данной Директиве предпринимается попытка унифицировать минимальные обязательства по хранению данных, которые возлагаются на провайдеров услуг электронной связи, действующих в государствах – членах Европейского союза, в целях предупреждения, расследования и раскрытия уголовных преступлений, а также судебного преследования за их совершение.

411. Директива 2006/24/ЕС обязывает государства-члены принять законодательство[178], требующее от провайдеров услуг электросвязи сохранять определенные виды данных о потоках электронных сообщений[179] в течение периода от шести месяцев до двух лет. Эти данные о потоках сообщений включают информацию, необходимую для идентификации отправителя и получателя интернет-почты и сообщений по каналам телефонной связи, а также сведения о времени, дате и продолжительности этих сеансов связи, но не распространяются на содержание электронных сообщений[180]. В связи с расследованием и раскрытием серьезных преступлений и судебным преследованием за их совершение такие данные должны предоставляться в распоряжение национальных правоохранительных органов и, при посредстве компетентных национальных органов[181], их коллегам в других государствах – членах Европейского союза, в соответствии с требованиями соответствующих национальных законов.

412. Например, после того как положения Директивы будут перенесены в национальное законодательство и при условии соблюдения применимых процессуальных требований национальные правоохранительные органы могут потребовать от провайдеров услуг предоставления доступа к данным в целях идентификации абонентов, использующих конкретные

[175] European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)", document COM(2011) 225 (Brussels, 18 April 2011), sect. 3.2.

[176] *Official Journal of the European Union*, L 105, 13 April 2006.

[177] Ibid., preamble, para. 6.

[178] По состоянию на апрель 2011 года законодательство о ее введении в действие вступило в силу в 22 государствах – членах Европейского союза.

[179] Это касается данных, генерируемых или обрабатываемых провайдерами услуг в ходе их деятельности, например в целях передачи сообщений, выставления счетов, установления соединений, получения оплаты, маркетинга и предоставления некоторых других дополнительных видов обслуживания.

[180] *Official Journal of the European Union*, L 105, 13 April 2006, art. 5.

[181] Ibid., art. 4.

IP-адреса, и тех, с кем эти лица вступали в контакт в течение заданного периода времени[182], Кроме того, при расследовании террористических актов сохраняемые провайдерами услуг данные, отражающие временны*е* затраты на планирование такого акта, могут использоваться для выявления моделей преступного поведения и отношений между соучастниками преступления, а также для установления наличия преступного умысла[183]. Некоторые государства – члены Европейского союза[184] отмечают, что протоколы сохранения данных являются единственным средством расследования некоторых преступлений, связанных с такими формами обмена информацией через Интернет, как передача сообщений на чат-форум, которые можно проследить только по данным об интернет-трафике[185]. Несколько государств – членов Европейского союза[186] также сообщили о случаях использования сохраняемых провайдерами услуг данных, чтобы снять подозрения с лиц, которые подозревались в совершении преступлений, не прибегая к другим, более интрузивным методам контроля, таким как перехват сообщений и обыск жилища. Не менее важны данные о местонахождении, которые сотрудники правоохранительных органов используют в целях исключения присутствия подозреваемых на месте преступления, а также для проверки алиби. Данные, сохраняемые в соответствии с законодательством о введении положений Директивы в силу, также позволяют выстраивать цепочки доказательств вплоть до момента совершения террористического акта, в том числе способствуя выявлению или подтверждению других видов улик, свидетельствующих о деятельности подозреваемых и связях между ними[187].

2. Веб-сайты и другие платформы, предоставляющие услуги по размещению пользовательского контента

413. Связанный с терроризмом контент, в случае его размещения на содержащих пользовательский контент популярных веб-сайтах, получает потенциальную возможность привлечь к себе внимание значительно более широкой аудитории, чем содержимое традиционных специализированных веб-сайтов, досок объявлений и форумов, которые обычно ориентированы лишь на группы лиц, которых объединяют собственные узкие интересы. По данным предназначенного для обмена видео веб-сайта YouTube, на него каждую минуту поступают пользовательские видеоматериалы объемом 48 часов, в результате чего ежедневно загружается контент, по продолжительности эквивалентный почти восьми годам[188]. Поскольку YouTube предоставляет этот контент в распоряжение порядка 8 млн. индивидуальных пользователей в месяц, это существенно снижает барьеры для доступа к контенту, связанному с терроризмом. Отмечаемый в последние годы резкий рост популярности пользовательского контента ведет к увеличению трудностей материально-технического характера в сфере контроля за контентом, связанным с терроризмом. Кроме того, пользователи веб-сайтов, предоставляющих услуги по размещению видеоматериалов, могут случайно натолкнуться на контент, связанный с терроризмом, в результате поиска или просмотра материала более умеренного характера, поскольку встроенные механизмы автоматически предлагают ознакомиться с материалами, сходными по содержанию.

[182] European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)", sect. 5.2.

[183] Ibid., sects. 3.1 and 5.2.

[184] Бельгия, Ирландия и Соединенное Королевство.

[185] European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)", sect. 5.4.

[186] Германия, Польша, Словения и Соединенное Королевство.

[187] European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)", sect. 5.4.

[188] Статистические данные по YouTube см. по адресу: www.youtube.com/t/press_statistics.

Дело Филиц Г.

По данному делу, слушавшемуся в Германии, подсудимая Филиц Г. была признана виновной по обвинениям в вербовке членов или сторонников для иностранных террористических организаций (групп "Аль-Каида", "Союз исламского джихада" и "Немецкие талибы-моджахеды") и оказании поддержки этим организациям.

В марте 2009 года обвиняемая присоединилась к интернет-форуму и начала публиковать в переводе на немецкий язык коммюнике террористических организаций с осуждением якобы имевших место преступлений международных вооруженных сил в Ираке и Афганистане и призывами к пользователям присоединиться к джихаду или поддержать его. Поскольку Филиц Г. являлась супругой находившегося в заключении немецкого террориста, она вскоре получила права администратора этого интернет-форума. К моменту своего ареста в феврале 2010 года обвиняемая поместила более 1000 сообщений и комментариев как в общедоступной части интернет-форума, так и в его закрытом разделе, предназначенном только для зарегистрированных пользователей. Филиц Г. открыла девять видеоканалов на портале YouTube и разместила на всех этих каналах 101 видеоматериал, включая как публикации террористических групп, таких как "Аль-Каида" и "Союз исламского джихада", так и видео, подготовленные ею самой. Обвиняемая очень тесно взаимодействовала с М., "координатором по работе со средствами массовой информации" из группы "Союз исламского джихада". Он связался с ней через Интернет и первоначально попросил ее перевести тексты религиозного содержания с турецкого языка на немецкий. Впоследствии он передал ей ссылки на видео, которые обвиняемая разместила на YouTube, и попросил ее оказать помощь в сборе пожертвований.

В одном случае обвиняемая перевела на немецкий язык материал, который был опубликован на веб-странице, выпускаемой на турецком языке, и поместила его на немецкой веб-странице. Данный материал представлял собой призыв к донорам оказать поддержку "семьям моджахедов в Афганистане, которые противостоят жестоким нападениям государств, развязавших против них крестовый поход". Текст сопровождался семью фотографиями, на одной из которых были изображены различные продукты питания, а на других шести – дети, вооруженные автоматами и другими видами оружия.

Помимо публикации материалов в поддержку сбора средств, обвиняемая также участвовала в фактическом сборе средств. В целях сохранения анонимности доноров она завела абонементный почтовый ящик, на который доноры адресовали конверты, подписанные их именами пользователей Интернета и содержавшие денежные средства (как правило, пожертвования в размере нескольких сотен евро). Затем, пользуясь услугами компании Western Union Financial Services, она переводила эти деньги посреднику в Турции, который пересылал их М., находившемуся в Вазиристане. Обвиняемая также размещала в Интернете видео, в которых благодарила доноров (для этой цели им присваивались псевдонимы, связанные с их именами пользователей Интернета) и информировала их о ходе кампании по сбору средств.

На суде в марте 2011 года подсудимая признала свою вину и была приговорена к лишению свободы сроком на два с половиной года. Вынося ей приговор, суд обосновал его тем, что обвиняемая полностью сознавала, что распространявшиеся ею пропагандистские материалы исходили от террористических организаций и что собранные и переданные ею средства предназначались для закупки, помимо гуманитарных товаров, также оружия и боеприпасов для этих организаций. Отметив, что данные преступления совершались преимущественно с использованием Интернета, выносящий приговор судья заявил:

> […] Суд придает особое значение существенной опасности распространения джихадистской пропаганды через Интернет. После того как материалы загружены в Интернет, их практически больше невозможно контролировать или удалить из Сети, поскольку другие пользователи могут их скачать, использовать и распространить дальше. Учитывая почти всемирный охват этой информационной среды, а также чрезвычайно большое и постоянно растущее число ее пользователей, Интернет представляет собой платформу, приобретающую все большее значение для террористических групп как средство распространения их целей и пропагандистских материалов и создания во всем мире атмосферы страха перед вездесущими террористическими угрозами. Таким образом, распространение материалов, подобных тем, которые публиковала обвиняемая, равноценно "интеллектуальному поджигательству". Данная деятельность имеет несравнимо более долгосрочный эффект и, следовательно, более опасна, чем, например, распространение пропаганды в виде листовок и других печатных средств массовой информации.

414. Возбужденное в Соединенном Королевстве дело *Государство против Рошанары Чоудри* является примером террориста-самоучки, г-жи Чоудри, радикализация которой, толкнувшая ее на совершение насильственных действий, происходила исключительно благодаря материалам, доступ к которым она получала через Интернет, и в частности с помощью веб-сайтов, специализирующихся на размещении видео. Дело г-жи Чоудри заставило международное сообщество обратить внимание на ту легкость, с которой платформа для обмена видеоматериалами, на которой содержался создаваемый пользователями контент, позволяла ей находить и просматривать видео экстремистского исламистского содержания, и на процесс, посредством которого убеждения, побудившие ее совершить террористический акт, сформировались в результате постоянного просмотра такого контента на протяжении нескольких месяцев.

415. В 2010 году, после обсуждений с правительствами Соединенного Королевства, которое представляла созданная на базе правоохранительных ведомств Группа реагирования на просьбы о помощи в борьбе с терроризмом в Интернете, и Соединенных Штатов, где находятся серверы YouTube, корпорация Google Inc., являющаяся компанией – учредителем YouTube, добровольно ввела систему, которая дала возможность пользователям контента помечать потенциально связанный с терроризмом контент на веб-сайте YouTube. Этот механизм является важным средством упреждающего выявления контента, который может способствовать совершению террористических актов.

416. Некоторые веб-сайты и платформы социальных сетей также включают в свои правила пользования положения, запрещающие использование их услуг в целях содействия, в частности, террористической деятельности. Например, правила пользования сервисом Twitter[189], сетью для обмена информацией в режиме реального времени, запрещают использование этого сервиса для публикации прямых, конкретных угроз насилием в отношении других лиц, или в любых других противозаконных целях, или для содействия противозаконной деятельности[190]. В случае нарушения этих условий провайдер услуг оставляет за собой право (хотя и не несет обязанности) удалить противоправный контент или отказаться от его распространения либо прекратить обслуживание абонента. Кроме того, круг пользователей Twitter ограничен лицами, которым не запрещено пользоваться услугами согласно законодательству Соединенных Штатов или иной соответствующей юрисдикции, таким образом исключается

[189] См. по адресу: https://twitter.com/tos.

[190] См. http://support.twitter.com/articles/18311-the-twitter-rules#.

возможность использования его услуг установленными террористическими организациями. Тем не менее даже при наличии таких правил могут возникать трудности с их применением, отчасти из-за масштаба пользовательской базы и, соответственно, большого объема подлежащего мониторингу пользовательского контента.

417. В новостных сообщениях последнего времени отмечается, что в случаях нарушения авторских прав компания Google нередко принимает меры по удалению противозаконного контента или ссылок на него в течение шести часов после получения просьбы об этом, несмотря на то что в 2011 году компанию просто засыпали запросами, касавшимися такого контента (было получено более 5 млн. таких запросов)[191]. Сочетание механизма, позволяющего помечать контент, и столь же настойчивого и своевременного реагирования в связи с подозрениями, что тот или иной контент имеет отношение к терроризму, было бы очень позитивным шагом вперед в борьбе с использованием Интернета для вербовки, радикализации, обучения, а также прославления терроризма и подстрекательства к совершению террористических актов.

418. Распространяемый террористическими организациями контент часто бывает отмечен "фирменными знаками", ассоциированными с конкретными организациями[192]. Мониторинг и удаление такого легко идентифицируемого контента разместившими его веб-сайтами могли бы обеспечить значительные успехи в борьбе с противозаконным распространением террористической пропаганды. Кроме того, использование механизмов, позволяющих помечать контент, аналогичных введенному на сервисе YouTube, в качестве стандартной функции по всему спектру социальных сетей и поисковых систем в Интернете может привести к повышению вероятности своевременного удаления пропагандистских материалов, направленных на содействие достижению террористических целей. Расширение мер по выявлению связанного с терроризмом контента в сочетании с активизацией формирования официальных и неофициальных партнерств по обмену информацией между заинтересованными сторонами в государственном и частном секторах могло бы существенным образом способствовать выявлению и противодействию террористической деятельности, связанной с использованием Интернета.

419. Обмен информацией особенно важен в контексте разграничения между онлайн-контентом, который может вызывать неодобрение или возражения, и контентом, который может быть противозаконным (см. обсуждение в разделе B.1 главы I). Например, хотя используемая на YouTube система маркировки контента может помочь в выявлении определенного контента, подлежащего анализу в первую очередь, далее возникает необходимость установить, отвечает ли такой контент необходимым критериям, позволяющим его удалить или заблокировать. Упростить этот процесс может неофициальный диалог между провайдерами услуг Интернет и веб-сайтами, предоставляющими услуги по размещению контента, с одной стороны, и сотрудниками органов уголовного правосудия, с другой. В этих целях можно побуждать соответствующие заинтересованные организации в частном секторе к сотрудничеству с правоохранительными органами путем предоставления информации о вызывающем возражения контенте, в отношении которого имеются подозрения, что он имеет отношение к кому-либо из пользователей, связанных с известными террористическими организациями или содействующих деятельности таких организаций.

[191] Jenna Wortham, "A political coming of age for the tech industry", *The New York Times*, 17 January 2012. См. по адресу: www.nytimes.com/2012/01/18/technology/web-wide-protest-over-two-antipiracy-bills.html?hp.

[192] "Jihadist use of social media: how to prevent terrorism and preserve innovation", testimony of A. Aaron Weisburd, Director, Society for Internet Research, before the United States House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, 6 December 2011.

3. Поисковые службы в Интернете

420. Поисковые службы в Интернете являются связующим звеном между интернет-контентом и конечным пользователем. Исключенный из таких поисковых систем контент имеет значительно меньшую аудиторию. Некоторые интернет-поисковики, такие как Google и Yahoo, добровольно подвергают цензуре контент, считающийся подозрительным или наносящим ущерб их интересам. Например, после террористических актов в Соединенных Штатах 11 сентября 2001 года многие поисковые системы в Интернете удалили результаты поисков, относящиеся к потенциальным террористическим организациям[193]. Разработчики политики и сотрудники правоохранительных органов в ряде государств-членов поощряют подобные добровольные инициативы, чтобы затруднить доступ через поисковые системы Интернета к контенту, который может способствовать совершению актов насилия. Полезной может также оказаться добровольная реализация поисковыми службами систем маркировки контента, связанного с терроризмом, подобных тем, что используются на YouTube.

4. Службы мониторинга

421. Некоторые частные субъекты также придерживаются более структурированного подхода к противодействию террористической деятельности в Интернете. Службы контроля, такие как базирующаяся в Соединенных Штатах Служба поиска международных террористических организаций (SITE) и сеть "Интернет-Хагана", ведут мониторинг и сбор касающейся террористических организаций информации из открытых источников[194]. Служба поиска международных террористических организаций, функционирующая как служба по сбору разведывательной информации, получает значительные доходы за счет платных подписок. Таким образом, данная Служба как таковая и подобные ей организации могут иметь более эффективный доступ к ресурсам для скорейшего выявления и перевода, когда это необходимо, материалов о деятельности в Интернете, которая может способствовать совершению террористических актов. "Интернет-Хагана", напротив, отслеживает деятельность исламистских экстремистских групп в Интернете в целях выявления контента, связанного с терроризмом, и пресечения доступа к нему. "Интернет-Хагана" частично финансируется за счет пожертвований и работает главным образом на основе участия сети добровольцев. Эта служба мониторинга работает на упреждение, исследуя и выявляя интернет-контент, считающийся связанным с терроризмом, и соответствующие веб-сайты, на которых он размещается. Данная служба может делиться такой информацией с правоохранительными органами или общественностью либо использовать ее для установления контактов с веб-сайтом, разместившим такой контент, чтобы способствовать его удалению или прекращению доступа к нему[195]. Хотя цели и способы функционирования этих служб мониторинга различаются, обе они своими действиями способствуют быстрому выявлению связанного с терроризмом контента в Интернете, что может быть полезно для сбора разведывательной информации, а также для расследования такого рода деятельности и судебного преследования за нее.

B. Партнерство государственного и частного секторов

422. Создание направленных на противодействие использованию Интернета в террористических целях партнерств между заинтересованными сторонами в государственном и частном секторах может принести немало потенциальных преимуществ. Как правило, среди проблем на пути развития сотрудничества между государственным и частным сектором в области

[193] Conway, "Terrorism and Internet governance: core issues", p. 30.

[194] Ibid, p. 31.

[195] Ariana Eunjung Cha, "Watchdogs seek out the web's bad side", *Washington Post*, 25 April 2005. См. по адресу: www.washingtonpost.com/wp-dyn/content/article/2005/04/24/AR2005042401473.html.

борьбы с киберпреступностью нередко упоминают о недостаточности контактов между правоохранительными органами и провайдерами услуг Интернет по вопросам обеспечения эффективного сбора улик, а также о противоречиях между принципом неприкосновенности частной жизни и необходимостью сохранения данных в правоприменительных целях. Создание форума для ведения официального и неофициального диалога между партнерами из государственного и частного секторов могло бы существенно снизить остроту таких проблем. Помимо возможностей, открывающихся благодаря проведению регулярных встреч между участвующими партнерами, помочь в устранении барьеров для поддержания связей и дальнейшего укрепления доверия между соответствующими участниками таких партнерств также могли бы такие мероприятия, как организация совместных учебных программ[196].

423. Значительный прогресс был достигнут в создании партнерств между государственным и частным сектором по вопросам обеспечения безопасности, связанным с потенциальными террористическими атаками на уязвимые объекты или инфраструктуру либо в связи с предотвращением и уголовным преследованием киберпреступности в целом. Полезным было бы также создание аналогичных государственно-частных партнерств в связи с регулированием использования Интернета в террористических целях. Примером успешного государственно-частного партнерства, связанного с обеспечением безопасности, является Консультативный совет по вопросам безопасности за рубежом, созданный совместно Государственным департаментом Соединенных Штатов и американскими организациями частного сектора, ведущими операции за границей. Совет служит форумом для обмена передовым опытом, а также платформой для регулярного и своевременного обмена информацией между частным сектором и правительством Соединенных Штатов относительно событий в сфере безопасности за рубежом, в том числе в связи с деятельностью террористов, а также политических, экономических и социальных факторов, которые могут воздействовать на состояние безопасности в глобальном масштабе и по отдельным странам[197].

424. Индонезийская Группа реагирования на инциденты, связанные с безопасностью инфраструктуры Интернета, является еще одним примером инициативы по созданию партнерства между государственным и частным сектором, в центре внимания которого находятся вопросы обеспечения безопасности. Она объединяет представителей служб почты и электросвязи, национальной полиции, Генеральной прокуратуры, Банка Индонезии, Индонезийской ассоциации провайдеров услуг Интернет, Индонезийской ассоциации интернет-кафе, Индонезийской ассоциации эмитентов кредитных карт и Индонезийского общества ИКТ (MASTEL). Ее члены сотрудничают в том числе в целях проведения мониторинга, обнаружения проблем и сбоев в телекоммуникационных сетях на основе протокола Интернет и раннего оповещения о них; осуществления исследований и разработок; организации лабораторного моделирования и профессиональной подготовки по вопросам безопасного использования телекоммуникационных сетей на основе протокола Интернет; предоставления консультативных услуг и технической помощи стратегически важным ведомствам или учреждениям; а также выполнения функций координационного центра для соответствующих ведомств или учреждений, как внутренних, так и международных[198].

425. В ноябре 2006 года в Москве был созван Глобальный форум по партнерству государств и бизнеса в противодействии терроризму. По итогам этого форума Группа восьми[199] приняла

[196] Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия, Партнерства государственного и частного секторов для защиты уязвимых объектов от атак террористов: обзор деятельности и выводы (январь 2009 года), пункт 23.

[197] Там же, пункт 9.

[198] Письменный материал, представленный экспертом от Индонезии.

[199] Неофициальный форум глав следующих промышленно развитых стран: Германии, Италии, Канады, Российской Федерации, Соединенного Королевства, Соединенных Штатов, Франции и Японии.

Стратегию партнерства государств и бизнеса в противодействии терроризму[200], направленную на поощрение, в частности, сотрудничества между провайдерами услуг Интернет и другими коммерческими компаниями и государственными ведомствами в борьбе с неправомерным использованием Интернета террористами и в целях не допустить подталкивания к последним шагам, которые ведут от экстремизма к терроризму. В рамках данной Стратегии правительствам предлагается на добровольной основе наладить более тесные национальные и международные партнерские связи с провайдерами услуг Интернет в целях решения проблем, связанных с использованием Интернета для таких видов деятельности, как вербовка, обучение и подстрекательство к совершению террористических актов.

426. К числу других значимых инициатив по созданию партнерств между государственным и частным сектором относится учрежденная в 2007 году рабочая группа Совета Европы с участием представителей правоохранительных органов, промышленности и ассоциаций провайдеров услуг Интернет для решения вопросов, связанных с киберпреступностью в целом. Цель этой инициативы состоит в укреплении сотрудничества между правоохранительными органами и частным сектором, для того чтобы более эффективно вести борьбу с киберпреступностью.

427. В 2010 году Европейская комиссия одобрила и предоставила финансирование для проекта, предполагающего установление сотрудничества между академическими кругами, промышленностью и правоохранительными органами и направленного на создание в Европе сети центров повышения квалификации для профессиональной подготовки, научных исследований и образования в области борьбы с киберпреступностью (2CENTRE). В настоящее время данная сеть обеспечивает обучение через национальные центры повышения квалификации, находящиеся в Ирландии и Франции. Каждый национальный центр основан на партнерстве между представителями правоохранительных органов, промышленных и научных кругов, которые взаимодействуют друг с другом в разработке соответствующих программ обучения и инструментария для использования в борьбе с киберпреступностью (см. раздел G главы IV).

428. Партнерства между государственным и частным сектором, специально направленные против использования Интернета террористами, могли бы также служить средством содействия распространению четких руководящих принципов в отношении обмена информацией между частным и государственным сектором, отвечающего применимым правилам защиты данных. Хорошей основой для формулирования руководящих принципов в области обмена информацией являются принятые Советом Европы "Руководящие принципы сотрудничества правоохранительных органов и провайдеров услуг сети Интернет против компьютерных преступлений"[201]. Основное внимание в этих Руководящих принципах уделяется установлению отношений взаимного доверия и сотрудничества между заинтересованными сторонами в государственном и частном секторах в качестве фундамента для их взаимодействия. В Руководящих принципах также подчеркивается необходимость содействия принятию действенных и экономически эффективных процедур сотрудничества. Правоохранительным органам и провайдерам услуг Интернет предлагается в целях расширения своих возможностей по выявлению киберпреступности и борьбы с ней принимать участие в обмене информацией путем проведения регулярных встреч, обмена передовым опытом и поддержания обратной связи. В Руководящих принципах также рекомендуется создавать официальные партнерства и использовать письменные процедуры в качестве основы для установления долгосрочных отношений в целях, в частности, обеспечения надлежащих гарантий того, что партнерство

[200] A/61/606-S/2006/936, приложение.

[201] Совет Европы, Отдел проблем экономической преступности, Руководящие принципы сотрудничества правоохранительных органов и провайдеров услуг сети Интернет против компьютерных преступлений (Страсбург, 2 апреля 2008 года). См. по адресу: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

не будет ущемлять законные права участников от частного сектора или правомочия правоохранительных органов[202].

429. Рекомендуемые меры, которые в соответствии с этими Руководящими принципами должны принять правоохранительные органы, включают:

- участие в широкомасштабном стратегическом сотрудничестве с провайдерами услуг Интернет, в том числе путем регулярного проведения учебных семинаров по техническим и правовым вопросам, а также обеспечение обратной связи в отношении проведенных расследований или собранной разведывательной информации на основе сообщений/жалоб со стороны провайдера услуг;

- предоставление разъяснений и помощи провайдерам услуг Интернет в отношении методов следствия, прямо не связанных с текущим делом, в целях содействия пониманию провайдерами услуг того, каким образом их содействие поможет повысить эффективность расследования;

- установление приоритета запросов на большие объемы данных и избежание ненужных затрат и создания помех для ведения деловых операций[203].

430. Рекомендуемые меры, которые в соответствии с этими Руководящими принципами должны быть приняты провайдерами услуг Интернет, включают:

- сотрудничество в целях сведения к минимуму использования услуг в противозаконных целях;

- информирование правоприменительных органов о преступной деятельности;

- предоставление, по возможности и при наличии соответствующего запроса, списка с указанием того, какие типы данных могут быть предоставлены правоохранительным органам по каждой услуге в случае получения надлежащим образом оформленного требования о раскрытии информации[204].

431. Проекты партнерства государственного и частного секторов могут также послужить форумом для содействия распространению минимальных стандартов надежного хранения данных заинтересованными сторонами в частном секторе и повышению эффективности каналов связи для предоставления заинтересованными сторонами в частном секторе информации относительно вызывающей подозрения деятельности.

[202] Там же, пункты 10–13.

[203] Там же, пункты 17, 29, 30 и 33.

[204] Там же, пункты 41, 42 и 50.

VIII. Заключение

A. Использование Интернета в террористических целях

432. Во вводных главах настоящего документа представлен построенный по функциональному принципу обзор средств, с помощью которых Интернет нередко используется в целях поощрения и поддержки террористических актов, в частности в плане пропаганды (в том числе в целях вербовки, радикализации и подстрекательства к терроризму), обучения боевиков и финансирования, планирования и осуществления таких актов. Большое внимание также уделяется возможностям, которые Интернет открывает для предупреждения, отслеживания и пресечения актов терроризма. К их числу можно отнести сбор разведывательной информации и иные виды деятельности, направленные на предотвращение и пресечение террористических актов, а также сбор доказательств в целях судебного преследования за совершение таких актов.

433. В целях пресечения процесса радикализации и насаждения экстремистских идеалов, которые, в свою очередь, могут быть продемонстрированы путем совершения террористических актов, могут использоваться такие эффективные средства, как контрпропаганда и распространение различных сообщений стратегического характера. В целях проведения конструктивного диалога с потенциальными кандидатами для вербовки в ряды террористов и пропагандирования альтернативных, правомерных средств достижения законных политических, социальных или религиозных устремлений также крайне важно показывать понимание лежащих в основе радикализации широких проблем.

434. Неотъемлемой частью борьбы с терроризмом является осуществление прав человека и принципа верховенства права. В частности, государства-члены вновь подтвердили эти обязательства в Глобальной контртеррористической стратегии Организации Объединенных Наций, признав, что "действенные меры по борьбе с терроризмом и защита прав человека являются целями, которые не противоречат, а дополняют и взаимно подкрепляют друг друга". На всех этапах реализации инициатив по борьбе с терроризмом – от сбора разведывательной информации в превентивных целях до обеспечения надлежащей правовой процедуры в ходе уголовного преследования подозреваемых – необходимо постоянно проводить оценки эффективности применения подхода к борьбе с использованием Интернета в террористических целях на основе принципа верховенства права.

B. Международный контекст

435. В настоящее время не существует всеобъемлющего договора Организации Объединенных Наций по борьбе с терроризмом, как не существует и официального определения термина "терроризм". Тем не менее государства – члены Организации Объединенных Наций находятся в процессе разработки проекта всеобъемлющей конвенции о международном терроризме, которая дополнит существующую международно-правовую базу в области борьбы с терроризмом. Эту базу составляет ряд различных источников, включая резолюции Генеральной Ассамблеи и Совета Безопасности, договоры, судебную практику и международное обычное право. Полезные материальные и процессуальные нормы, касающиеся криминализации террористических актов, которые могут совершаться с использованием Интернета, также содержатся в нескольких региональных и субрегиональных документах.

436. В соответствии с Глобальной контртеррористической стратегией государства-члены постановили принять незамедлительные меры по предотвращению терроризма и борьбе с ним во всех его формах и проявлениях, и в частности:

a) рассмотреть вопрос о присоединении без промедления в качестве сторон к существующим международным конвенциям и протоколам против терроризма и осуществлять их и приложить все усилия для согласования и заключения всеобъемлющей конвенции о международном терроризме;

b) осуществить все резолюции Генеральной Ассамблеи о мерах по ликвидации международного терроризма и соответствующие резолюции Генеральной Ассамблеи о защите прав человека и основных свобод в условиях борьбы с терроризмом;

c) осуществить все резолюции Совета Безопасности, касающиеся международного терроризма, и полностью сотрудничать со вспомогательными контртеррористическими органами Совета Безопасности в выполнении их задач.

C. Политика и законодательные рамки

1. Политика

437. Для принятия эффективных ответных мер со стороны органов уголовного правосудия в связи с угрозами, которые представляет использование Интернета террористами, от правительств требуется выработать четкую национальную политику и законы в отношении, в частности: *a)* криминализации противоправных действий, осуществляемых террористами через Интернет или связанные с ним сервисы; *b)* предоставления следственных полномочий правоохранительным органам, занимающимся расследованиями, связанными с терроризмом; *c)* регулирования услуг, связанных с Интернетом (например, деятельности провайдеров услуг Интернет), и контроля за контентом; *d)* содействия международному сотрудничеству; *e)* выработки специальных процедур судопроизводства или представления доказательств; а также *f)* поддержания международных стандартов в области защиты прав человека.

438. Предложенная Рабочей группой по противодействию использованию Интернета в террористических целях Целевой группы по осуществлению контртеррористических мероприятий широкая классификация стратегических подходов, предполагающая применение общего законодательства о борьбе с киберпреступностью, общего (не связанного непосредственно с использованием Интернета) законодательства о борьбе с терроризмом и законодательства о борьбе с терроризмом, конкретно связанного с использованием Интернета, является полезной концептуальной основой для разработчиков политики и законодателей. В настоящее время лишь в немногих государствах выработано законодательство, специально направленное на борьбу с деяниями, которые террористы совершают с использованием Интернета. Большинство стран используют для криминализации этих видов преступлений и уголовного преследования за их совершение общее уголовное законодательство и законодательство о борьбе с киберпреступностью и/или терроризмом.

2. Законодательство

439. Помимо использования Интернета в рамках действий, связанных с основными преступлениями (например, взрывами), террористы могут использовать Интернет для проведения других мероприятий вспомогательного характера (например, распространения пропагандистских материалов или вербовки и обучения боевиков). Страны применяют различные подходы к криминализации противоправных деяний, связанных с терроризмом, совершаемых при посредстве Интернета.

440. В своей резолюции 1624 (2005) Совет Безопасности, в частности, призвал государства ввести уголовную ответственность за подстрекательство к совершению террористических актов. Согласно этой резолюции и другим международным документам государства обязаны обеспечивать, чтобы меры, направленные против подстрекательства к терроризму, в полной мере соответствовали их международным обязательствам по праву в отношении прав человека, беженскому праву и гуманитарному праву.

441. Разработка и применение законов, криминализующих подстрекательство к совершению актов терроризма при полном обеспечении прав человека (например, права на свободу выражения мнения), остаются постоянной проблемой для разработчиков политики, законодателей, правоохранительных органов и органов обвинения во всех странах. Страны придерживаются различных подходов к криминализации актов подстрекательства к терроризму. В некоторых странах уголовная ответственность установлена непосредственно за подстрекательство к совершению террористических актов или их прославление, тогда как в других используются статьи, относящиеся к незавершенным преступлениям, таким как подстрекательство к совершению преступления или преступный сговор.

442. Расследование дел о терроризме, касающихся использования Интернета или других связанных с ним услуг лицами, подозреваемыми в террористической деятельности, нередко требует осуществления правоохранительными органами специальных видов следственных полномочий. Большинством правительств принято законодательство, позволяющее правоохранительным органам вести такую деятельность в рамках расследований, связанных с терроризмом. Для использования таких методов ведения расследования необходимо иметь надлежащие полномочия в соответствии с национальным законодательством; кроме того, они должны применяться таким образом, чтобы не нарушались основные права человека, защищаемые согласно международным нормам в области прав человека.

443. В целях проведения электронного мониторинга, прослушивания телефонных разговоров и применения других подобных методов расследования с использованием электронных средств компетентным органам потребуется содействие операторов электросвязи. Желательно, чтобы со стороны правительств была обеспечена четкая правовая основа для возложения соответствующих обязательств на стороны, принадлежащие к частному сектору, включая необходимые технические характеристики их сетей и способы погашения затрат, связанных с предоставлением такого рода возможностей.

444. Имеются свидетельства того, что для осуществления своей деятельности террористы пользуются услугами интернет-кафе; однако масштабы этой проблемы неизвестны. Некоторые правительства в интересах правоохранительных органов (в том числе в целях борьбы с терроризмом) возлагают на операторов интернет-кафе конкретные обязательства по сбору, хранению и предоставлению правоохранительным органам, по их запросу, фотографий, удостоверяющих личность, адресов и данных об использовании Интернета/подключениях своих клиентов. Существуют некоторые сомнения относительно целесообразности введения таких мер только применительно к интернет-кафе, в то время как имеются и другие формы общественного доступа в Интернет (например, в аэропортах, библиотеках, а также в точках беспроводного доступа), в отсутствие какого-либо регулирования предоставляющие преступникам (в том числе террористам) аналогичные возможности.

445. Вопрос о том, в какой степени правительства должны регулировать связанный с терроризмом контент в Интернете, остается открытым и требует установления баланса между интересами правоохранительных органов и соблюдением прав человека (например, права на свободу выражения мнения). Известны различные подходы к регулированию связанного с терроризмом информационного наполнения, и некоторые государства прибегают к механизмам строгого регулирования деятельности провайдеров услуг Интернет и других сопутствующих услуг, в том числе в некоторых случаях к использованию технических средств фильтрации или блокирования доступа к некоторым видам контента. Другие государства

придерживаются менее жестких подходов к регулированию, в большей степени полагаясь на саморегулирование в секторе информационного сообщества. Большинство провайдеров услуг Интернет, веб-хостинговых компаний, файлообменных сайтов и социальных сетей имеют соглашения об условиях сервиса, которые запрещают размещение определенных видов контента; часть связанного с терроризмом контента может противоречить этим договорным ограничениям.

D. Расследования и сбор информации

446. Эффективность расследований в отношении деятельности в Интернете зависит от сочетания традиционных следственных методов, знания доступного инструментария для ведения противозаконной деятельности с использованием Интернета и разработки методик, направленных на выявление, задержание и судебное преследование виновных в совершении таких деяний. Инициативный подход к стратегиям ведения следствия и специализированным вспомогательным средствам, опирающимся на использование развивающихся интернет-ресурсов, способствует эффективному выявлению данных и сервисов, которые способны принести расследованию максимальную пользу.

447. Существует ряд специализированных утилит и аппаратных средств, доступных следователям с соответствующим техническим образованием. В делах, связанных с получением цифровых улик, надлежит, по возможности, уделять должное внимание использованию стандартных процедур извлечения данных, чтобы способствовать изъятию максимального количества имеющихся улик и сохранению целостности источника данных, а также соблюдению режима охраны доказательств, чтобы обеспечить их допустимость в суде. Ввиду того что цифровые улики легко повредить, для их оценки, изъятия и исследования наиболее эффективно привлекать специально обученных экспертов-криминалистов.

E. Международное сотрудничество

448. Важным фактором при осуществлении уголовного преследования по многим делам о терроризме, в том числе связанным с некоторыми аспектами использования преступниками Интернета, является эффективное международное сотрудничество. Многие касающиеся терроризма и транснациональной организованной преступности международные, региональные, многосторонние и двусторонние документы обязывают государства выработать политику и законодательную основу, способствующие эффективному международному сотрудничеству при расследовании террористических актов или связанных с ними деяний в рамках организованной преступности и уголовном преследовании виновных. В настоящее время не существует касающегося киберпреступности или терроризма универсального документа, в соответствии с которым на государства налагались бы конкретные обязательства в отношении международного сотрудничества. Это препятствует эффективному международному сотрудничеству в ходе отдельных расследований и уголовных процессов по делам о терроризме.

449. Хотя официальные каналы международного сотрудничества остаются жизненно важными, на практике не меньшее значение также приобретают неофициальные каналы. Независимо от формы взаимодействия, ключевым элементом эффективного международного сотрудничества во многих случаях являются доверительные отношения между соответствующими национальными компетентными органами. Помимо сотрудничества в рамках официальных договоров или аналогичных правовых документов, очень важны также не основанные на договорах региональные или субрегиональные инициативы по укреплению сотрудничества правоохранительных органов. Страны, имеющие общие интересы в области обеспечения безопасности в конкретных сферах, могут заключать коллективные соглашения, предусматривающие обмен информацией и совместное использование разведывательных данных.

450. Существование национальной законодательной базы, предусматривающей действенное международное сотрудничество, является одним из основополагающих элементов эффективной структуры содействия международному сотрудничеству в расследовании и уголовном преследовании по делам о терроризме. Посредством такого законодательства во внутреннее право страны должны быть инкорпорированы закрепленные в универсальных документах по борьбе с терроризмом принципы в отношении сотрудничества и связанной с терроризмом транснациональной организованной преступности.

451. Хотя законодательство является одним из основополагающих компонентов любого эффективного режима международного сотрудничества, само по себе оно не решает проблему в целом. Важнейшее значение также имеет наличие обеспеченного надлежащими ресурсами и инициативного центрального органа, способного, используя все доступные каналы, содействовать взаимной правовой помощи. Не менее важны развитие и поддержание доверительных отношений с иностранными партнерами, участвующими в сотрудничестве в ходе трансграничных уголовных расследований.

452. Помимо официальных каналов сотрудничества, компетентным органам необходимо развивать и использовать имеющиеся неофициальные каналы двустороннего взаимодействия. Многие национальные правоохранительные ведомства содержат сети международных пунктов связи, которые оказывают значительную помощь, содействуя выполнению просьб о международном сотрудничестве. В универсальных документах по борьбе с терроризмом не содержится прямых упоминаний об использовании совместных следственных групп; однако такая стратегия сотрудничества полностью соответствует основополагающим принципам и духу тех положений, которые касаются международного сотрудничества. В некоторых странах, особенно в Европе, такой подход был с успехом применен при проведении ряда расследований, связанных с терроризмом.

453. Несмотря на усовершенствования, официальные процедуры оказания взаимной правовой помощи по уголовным делам все еще могут представлять собой длительный процесс, сопряженный со значительным количеством бюрократических формальностей. В случаях, касающихся сохранения интернет-данных, находящихся у провайдеров услуг в другой юрисдикции, компетентные органы могли бы на неофициальной основе обращаться за содействием в сохранении таких данных для целей расследования или судебного преследования за совершение уголовного преступления непосредственно к провайдерам услуг Интернет. В других ситуациях могут потребоваться осуществление права на принуждение или наличие санкции суда, например, в отношении сохранения, проведения обыска и выемки связанных с Интернетом данных для их представления и использования в качестве доказательств в ходе уголовного процесса.

454. Следователи и обвинители должны быть полностью осведомлены о потенциальной важности таких данных и необходимости как можно раньше принять меры к их сохранению таким образом, чтобы была гарантирована их допустимость в качестве потенциальных доказательств в ходе любого последующего судебного разбирательства. По мере возможности, национальные правоохранительные органы должны выработать, либо непосредственно с провайдерами услуг Интернет, либо со своими коллегами в других странах, четкие процедуры, с использованием как официальных, так и неофициальных элементов, направленные на обеспечение скорейшей фиксации и представления необходимых для проведения уголовного расследования данных об использовании Интернета.

455. Некоторые специалисты на совещании группы экспертов подчеркивали тот факт, что препятствием для обмена информацией нередко становится необходимость обеспечения защиты секретных материалов разведки со стороны компетентных национальных органов.

456. При рассмотрении возможности проведения связанных со сбором цифровых улик следственных действий в других юрисдикциях компетентным органам следует помнить о последствиях, которые действия такого рода могут иметь с точки зрения суверенитета

других государств. Во всех случаях, когда это возможно, компетентные органы, планирующие предпринять следственные действия в отношении лиц или предметов, находящихся в пределах другой юрисдикции, должны уведомить об этом своих зарубежных коллег в соответствующих странах и согласовать с ними такие действия.

457. Важными доказательствами по многим делам о терроризме неизбежно служат данные, связанные с Интернетом (например, об использовании сети Интернет клиентом). В таких случаях компетентные органы должны обеспечить сохранность соответствующих данных для их последующего использования в качестве доказательств в суде. В связи с этим важно иметь в виду различие между "хранением" данных (хранение данных провайдерами услуг Интернет согласно предусмотренному правилами обязательству) и "обеспечением сохранности" данных (сохранение данных на основании судебного приказа или разрешения). Во многих странах провайдеры услуг Интернет обязаны по закону хранить определенные виды касающихся сообщений данных в течение установленного периода времени. В результате на международном уровне существуют значительные расхождения в отношении конкретных видов данных, сохраняемых провайдерами услуг Интернет, и периодов времени, в течение которых они хранятся. Это может порождать проблемы в случаях, когда компетентным органам требуется использовать данные об обменах сообщениями, которые находятся в одной стране, в качестве доказательств по уголовному делу, которое ведется в другой стране.

458. Разработка общепризнанной нормативной базы, на основании которой на всех провайдеров услуг Интернет были бы возложены единообразные обязательства в отношении подлежащих хранению видов данных об использовании Сети клиентами и сроков их хранения, принесла бы значительную пользу правоохранительным и разведывательным органам, расследующим дела о терроризме. В отсутствие общепризнанного порядка хранения данных провайдерами услуг Интернет компетентным органам надлежит на возможно раннем этапе установить, имеются ли у провайдеров услуг Интернет данные, относящиеся к расследованию, и где они находятся, и как можно раньше предпринять шаги к их сохранению для возможного использования в качестве доказательств.

459. Насколько это возможно, компетентным органам следует установить неофициальные связи или заключить договоренности с провайдерами услуг Интернет (как внутри страны, так и за рубежом), у которых могут находиться представляющие интерес для правоохранительных органов данные, в отношении процедур предоставления таких данных для их использования в ходе проводимых правоохранителями расследований. В отсутствие таких неофициальных процедур компетентным органам в ходе расследования следует при первой же возможности установить контакт с иностранными контрагентами, если потребуется, по официальным каналам и с соответствующего разрешения суда, на предмет обеспечения сохранности таких данных.

460. С доказательственной точки зрения связанные с трансграничными расследованиями дела о терроризме добавляют дополнительные трудности к тому, что и без того уже можно считать сложной задачей для следователей и обвинителей, требуя от них обеспечить, чтобы методы, используемые для сбора улик (возможно, в одной или нескольких странах) и предъявления их в качестве доказательств на уголовном процессе, проводимом в другой юрисдикции, были полностью согласованы с применимыми законами и принципами во всех соответствующих юрисдикциях.

461. Критерий "двойной уголовной ответственности" (требование, чтобы деяния, к которым относятся запросы о выдаче и оказании взаимной правовой помощи, считались уголовно наказуемыми преступлениями в обоих государствах), нередко фигурирующий в большом количестве многосторонних и двусторонних документов по борьбе с терроризмом и транснациональной организованной преступностью, может вызывать трудности в уголовных делах, в том числе связанных с терроризмом, которые содержат какие-либо элементы международного сотрудничества.

462. В связи с делами о терроризме, в которых деяния, являющиеся составляющими элементами преступления, совершаются через Интернет, могут возникать сложные вопросы в отношении юрисдикции, особенно в случаях, когда подозреваемый правонарушитель, находясь в одной стране, использует для совершения части преступления интернет-сайты или услуги, предоставляемые провайдерами, которые находятся в другой стране. Такие дела охватывают лиц, постоянно проживающих в одной стране, которые создают и администрируют веб-сайты, используемые для пропаганды джихада и других актов насилия, связанных с терроризмом.

463. Не существует никаких обязательных норм международного права в отношении того, как государства должны вести себя в случаях, если более чем одно государство может претендовать на обладание юрисдикцией, которая позволяет возбудить судебное преследование в связи с преступлением, совершенным одним и тем же подозреваемым. Как правило, национальные компетентные органы для определения того, следует ли заявить о своей юрисдикции и осуществлять ее в данном конкретном случае, соотносят или взвешивают соответствующие факторы, включая степень, в которой различные юрисдикции связаны с предполагаемым преступлением. В случаях, когда имеют место коллизии претензий на обладание юрисдикцией, важно скорейшим образом установить сотрудничество между соответствующими центральными органами (чаще всего национальными органами уголовного преследования), что позволит разрешить эти проблемы.

464. Национальное законодательство о защите информации или неприкосновенности частной жизни нередко ограничивает возможности правоохранительных и разведывательных органов делиться сведениями с партнерами внутри страны и за рубежом. Достижение разумного баланса между правом человека на неприкосновенность частной жизни и законной заинтересованностью государства в эффективном расследовании преступлений и уголовном преследовании за их совершение является постоянной проблемой для правительств и в отдельных случаях, в том числе связанных с ответными мерами против терроризма, становится предметом обеспокоенности.

F. Уголовное преследование

465. Неотъемлемой частью универсальной правовой базы для борьбы с терроризмом – Глобальной контртеррористической стратегии Организации Объединенных Наций – является возлагаемое на государства обязательство отказывать в убежище и привлекать к ответственности лиц, совершивших террористические акты, где бы они ни происходили. Помимо необходимой законодательной базы, неотъемлемую часть эффективных ответных мер системы уголовного правосудия в борьбе с терроризмом составляет наличие в рамках национальных органов уголовного преследования институционального потенциала для поддержания верховенства права и, в соответствии с международными нормами в области прав человека, обеспечения в ходе судебных процессов по делам, связанным с терроризмом, гарантий соблюдения прав человека подозреваемых и обвиняемых.

466. В делах о терроризме обвинители зачастую участвуют не только на этапе судопроизводства, но и играют непосредственную роль на этапе расследования, консультируя по правовым и стратегическим вопросам, которые будут влиять на исход любого возбужденного по результатам следствия судебного дела. Как правило, они выполняют эту роль в рамках междисциплинарной/межведомственной группы. Высокий уровень доверия, координации и контактов, жизненно важный для эффективного сотрудничества на международном уровне, должен существовать также и между национальными органами охраны правопорядка, разведки и уголовного преследования.

467. В то время как новые методы ведения расследования открывают перед компетентными органами более широкие возможности в борьбе с террористической деятельностью

в Интернете, они также несут с собой юридические риски, что требует от обвинителей постоянной бдительности. Различия в национальных законах, касающихся сбора и допустимости доказательств, означают, что эти риски повышаются, когда деяния, к которым относятся полученные доказательства, имели место не в той юрисдикции, в которой будет проводиться суд.

468. В большинстве стран обвинители пользуются широкой свободой действий при решении вопросов о том, следует ли возбуждать уголовное дело и на основании каких обвинений это следует сделать. Такие решения нередко принимаются в соответствии с руководящими принципами или кодексами, которые предназначены обеспечивать справедливое, прозрачное и последовательное осуществление этих важных дискреционных полномочий и в которых часто предусматриваются соответствующие пороги с учетом доказательной обоснованности и общественных интересов.

469. Основной целью связанных с терроризмом расследований является обеспечение общественной безопасности. В некоторых случаях компетентные органы в целях предотвращения совершения террористических актов бывают вынуждены вмешаться прежде, чем будут получены достаточные доказательства для возбуждения уголовного преследования в связи с планируемыми, как подозревают органы власти, террористическими актами.

470. В таких ситуациях в целях обеспечения правового обоснования своих действий компетентным органам, возможно, придется вместо основных преступлений, связанных с планируемыми террористическими актами, использовать другие составы уголовных преступлений, в том числе такие, как подстрекательство к совершению преступления, преступный сговор, участие в преступном сообществе или оказание материальной поддержки террористам. Для того чтобы сорвать или раскрыть деятельность террористических групп, прежде чем будут совершены планируемые ими нападения или иные акции, можно также использовать другие статьи общеуголовного характера, связанные с мошенничеством либо владением или использованием запрещенных предметов (например, фальшивых удостоверений личности/проездных документов, оружия).

471. По многим делам о терроризме используемые стороной обвинения доказательства бывают основаны на разведывательной информации. В процессе борьбы с терроризмом для компетентных органов одной из существенных проблем остается интеграция разведывательной деятельности с системами уголовного правосудия, то есть каким образом компетентные органы могли бы защитить секретные разведывательные данные, являющиеся основой доказательств, одновременно выполнив обязательства по обеспечению справедливого судебного разбирательства и эффективной защиты обвиняемых, в том числе обязательство раскрыть перед стороной защиты все существенные части версии обвинения?

472. По делам о терроризме, связанным с использованием компьютеров или Интернета, важной частью версии обвинения неизбежно становятся цифровые улики. Использование доказательств такого рода неизменно порождает проблемы, связанные с допустимостью. Исключительно важно на протяжении всего расследования и уголовного преследования по делу уделять максимум внимания гарантиям того, чтобы методы, используемые для сбора, сохранения, анализа и представления цифровых улик, находились в полном соответствии с применимыми правилами доказывания или процессуальными нормами и следовали установившейся практике.

473. Органам обвинения обязательно будет необходимо убедить суд в надежности цифровых улик, в том числе методов их сбора, анализа и представления. Процедуры сохранения целостности доказательств называют "цепочкой ответственного хранения" или "цепочкой доказательств". Когда сбор таких доказательств ведется в одной юрисдикции для использования в ходе судебного разбирательства в другой, ситуация оказывается значительно сложнее и требует пристального внимания со стороны следователей и обвинителей. В случаях, когда

компетентным органам удается установить наличие и/или местонахождение соответствующих цифровых доказательств, им надлежит изучить средства (неофициальные и официальные) их получения и сохранения для использования в доказательственных целях. Выбранный канал должен обеспечивать допустимость доказательств в стране, где состоится суд.

474. Правовые принципы и процедуры, связанные со сбором и допустимостью доказательств в уголовном судопроизводстве, нередко различаются по юрисдикциям. При проведении трансграничных расследований значительная часть работы компетентных органов заключается в "согласовании" различных аспектов, связанных с доказательствами. Это может оказаться сложным, отнимающим много времени процессом, но при этом является критическим фактором успеха судебного преследования. Любые юридические недостатки методов сбора, сохранения, передачи или представления доказательств, которые в конечном счете используются в процессе судебного разбирательства, почти наверняка будут оспорены защитой.

475. По делам о терроризме нередко, чтобы доказать тот или иной специальный (специальные) аспект (аспекты), обвинители прибегают к свидетельским показаниям экспертов. К числу областей, в которых часто требуются показания экспертов, относятся технологии и коммуникации, а также идеология, деятельность и организационная структура террористических групп. Вполне вероятно, что обвинителям может потребоваться несколько свидетелей-экспертов. Как правило, в связанных с использованием свидетелей-экспертов случаях выделяют три этапа или фазы: *a)* четкое определение проблем (и их рамок), в отношении которых требуется экспертное заключение; *b)* поиск квалифицированного специалиста; и *c)* обеспечение того, чтобы квалифицированный специалист использовал средства, допустимые в суде.

476. Обвинители должны на как можно более раннем этапе определить вопросы, по которым, по-видимому, потребуются показания экспертов, и дать экспертам поручение провести необходимый анализ, предоставив, если потребуется, четкие инструкции в отношении ключевых правил процедуры или доказывания. При выборе свидетелей-экспертов обвинителям следует решить, использовать ли государственных или негосударственных специалистов. Хотя использование государственных экспертов дает некоторые преимущества, использование негосударственных экспертов, возможно, желательнее в тех случаях, когда в качестве основы для их доказательств были использованы секретные разведывательные источники или методы. Поиск подходящего эксперта, особенно в узкоспециализированных областях, может представлять серьезную проблему для менее развитых стран. Во всех случаях, когда это возможно, свидетелям-экспертам надлежит следовать признанной установившейся практике в тех конкретных областях, в связи с которыми их вызвали. Ввиду сложности некоторых свидетельских показаний экспертов следует уделить внимание инновационным способам представления сложных доказательств судьям, присяжным или иным лицам, призванным устанавливать факты в ходе судебного разбирательства, в доступной форме. Важно, чтобы обвинитель обладал основательными практическими знаниями в конкретной предметной области.

477. Сложность многих судебных процессов по делам о терроризме, особенно связанных с международным сотрудничеством или сугубо техническими элементами, делает крайне желательным, чтобы дела велись группами обвинителей. В целях обеспечения комплексного подхода с позиций принципа верховенства права и сохранения единообразия ответных мер со стороны системы уголовного правосудия в борьбе с терроризмом в странах должны непоколебимо и беспрерывно вестись процессы укрепления потенциала обвинителей для осуществления национального законодательства по борьбе с терроризмом и связанных с этим обязательств в области международного сотрудничества. В странах, где высок риск террористической деятельности, а институциональный потенциал служб уголовного преследования и других органов уголовного правосудия невелик, первоочередное внимание следует уделять наращиванию потенциала специалистов этих учреждений как в плане ведения уголовных дел, так и применительно к соответствующим механизмам международного сотрудничества.

G. Сотрудничество с частным сектором

478. Хотя ответственность за противодействие использованию Интернета в террористических целях в конечном счете лежит на государствах-членах, сотрудничество с основными заинтересованными сторонами в частном секторе имеет решающее значение для эффективного выполнения данной функции. Упреждающее взаимодействие с заинтересованными представителями частного сектора, такими как провайдеры услуг Интернет, веб-сайты, предоставляющие услуги по размещению пользовательского контента, и поисковые системы в Интернете, будет продолжать играть важную роль в деле ограничения доступности распространяемого через Интернет контента, связанного с терроризмом.

479. В связи с регулированием использования Интернета в террористических целях полезным было бы создание партнерств между государственным и частным сектором. Похожие инициативы были с успехом разработаны применительно к другим областям противодействия терроризму и борьбы с киберпреступностью в целом. Инициативы такого рода ведут к созданию форума для официального и неофициального диалога между партнерами из государственного и частного секторов, а также позволяют осуществлять такие вспомогательные мероприятия, как совместные учебные программы, которые могут содействовать ликвидации барьеров в общении и дальнейшему укреплению доверия и взаимопонимания, а также выработке участвующими членами партнерств единообразной практики.

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Vienna International Centre, PO Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

Издание Организации Объединенных Наций
Отпечатано в Австрии

V.12-57354 – May 2013 – 100