Organization for Security and Co-operation in Europe

Серия экспертных онлайн-форумов ОБСЕ по использованию Интернета террористами: угрозы, ответы и возможные будущие шаги

Отчет

Action against Terrorism Unit
Transnational Threats Department
OSCE Secretariat
Wallnerstrasse, 6 A-1010 Vienna
http://www.osce.org/atu

Содержание

I. Краткая информация

В 2012 году Антитеррористическое подразделение Департамента по противодействию транснациональным угрозам Секретариата ОБСЕ (ДПТУ/АТП) организовало четыре экспертных онлайн-форума с целью укрепления и дальнейшего стимулирования обмена информацией о последних тенденциях и спорах в отношении использования террористами Интернета, актуальных сложных вопросах, связанных с реагированием на такие угрозы, а также применимой передовой практике и вариантах политики.

Один из основных компонентов этой инициативы заключался в выработке вариантов того, как ОБСЕ может в дальнейшем дополнять международные усилия в данной области, используя свои существующие мандаты. Это стало особенно актуально теперь, когда государства-участники приняли Решение постоянного совета № 1063 «О консолидированной концептуальной базе ОБСЕ для борьбы с терроризмом» (декабрь 2012 г.), в котором противодействие использованию Интернета в террористических целях признается стратегическим направлением контртеррористической деятельности ОБСЕ.

В целом в этих мероприятиях приняли участие 140 специалистов, представлявших органы власти государств-участников, организации гражданского общества, научное и деловое сообщество. Эксперты приняли участие в обсуждениях, направив более 164 сообщений, в которых они остановились на основных темах в этой области и дали пояснения по ним, предлагая потенциальные решения, представляя передовой национальный опыт и соответствующие международные инициативы, а также предлагая свои взгляды на те сферы, в которых ОБСЕ может быть более активно задействована благодаря своим сравнительным преимуществам.[1]

II. Основные темы и рекомендации

- **Гармонизированная международная правовая система** крайне важна для того, чтобы привлекать к ответственности кибертеррористов. Кроме того, такая система является ключевым элементом международного сотрудничества в сфере поддержания правопорядка, не в последнюю очередь потому, что многие страны основывают свои режимы взаимной юридической поддержки на принципе «обоюдного признания соответствующего деяния преступлением». Согласованные на международном уровне, продуманные и отвечающие требованиям законы также являются наилучшей гарантией обеспечения не только безопасности и конфиденциальности, но и международного сотрудничества. Необходимо регулярно пересматривать национальные правовые системы в соответствии с изменениями, возникающими на международном уровне, чтобы учитывать быстрое развитие технологий.

[1] Мнения, выраженные экспертами, не всегда отражают взгляды Секретариата ОБСЕ. Несмотря на то, что были приложены все усилия для отражения в отчете всех мнений, в целях ясности и удобочитаемости эти высказывания пришлось суммировать в соответствии с основными сообщениями и темами!

- **Сотрудничество на уровне практикующих специалистов крайне важно**, особенно в условиях быстрого развития интернет-технологий и отсутствия гармонизированной международной правовой системы, поскольку оно позволяет своевременно реагировать на использование Интернета террористами. Сюда следует включить двухступенчатый подход: на первом уровне реагирования – уровне органов охраны правопорядка – должны быть задействованы скоростные линии коммуникации в режиме реального времени, а на судебном уровне сюда необходимо включить тщательно продуманные процессы, обеспечивающие пригодность свидетельств к использованию в суде. В более широком смысле государствам также необходимо рассмотреть вопрос о создании соответствующих координационных центров в рамках их дипломатических миссий для усиления сотрудничества. *ОБСЕ могла бы рассмотреть вопрос о сохранении своей роли платформы по распространению информации для практикующих специалистов, дополняющей механизмы, созданные другими международными организациями.*

- **Усилия по борьбе с использованием Интернета террористами должны носить превентивный характер и поддерживать открытость Интернета. Любые необходимые принудительные действия должны иметь узкую направленность.** Невозможно контролировать весь онлайн-контент террористического и криминального характера, лучше направить усилия на поддержание открытого Интернета, чем просто закрывать веб-сайты. Однако иногда необходимо принимать принудительные меры, особенно если соответствующие действия переходят за определенные границы, например, в случае подстрекательства к насилию или возникновения непосредственной угрозы. Такие меры, включающие блокирование веб-сайтов или удаление материалов, должны приниматься в соответствии с четко сформулированными национальными законами и международными обязательствами и принципами, в которых соблюдаются основные права и устанавливается то, какими угрозами оправдываются определенные меры. Кроме того, важно создать эффективную систему надзора, при которой пострадавшая сторона будет иметь возможность подать жалобу в случае неправомерного применения санкции. В разработку политики необходимо вовлекать население и гражданское общество и обращаться к ним за содействием. Это важно для того, чтобы объяснить, чего пытаются добиться власти, а также, чтобы избежать отрицательной реакции общественности, которая, в свою очередь, создает возможности для развития терроризма. Аналогичным образом, властям необходимо думать о том, как такие усилия повлияют на международное сотрудничество и расследования, ведущиеся в других юрисдикциях. *Такие организации как ОБСЕ могут стать идеальным местом для оценки потенциальных принудительных мер, не только в плане их совместимости с основными свободами, но и в отношении оценки издержек и выгод таких мер.*

- **Несмотря на то, что технологии могут помочь сбору данных, именно сведения, получаемые в результате объединения информации, поступающей из многочисленных источников, включая государственные и прочие службы, позволяют составить наиболее полную картину.** В периоды бюджетных ограничений специально обученный персонал, способный анализировать постоянно растущие объемы передаваемых данных, должен работать максимально эффективно и, что

особенно важно, принимать во внимание человеческий фактор. Несмотря на то, что власти способны собирать огромные объемы данных, технические возможности целенаправленной тщательной проверки таких данных развиваются не столь быстрыми темпами, и в результате невозможно обойтись без человеческого вмешательства и анализа. С помощью таких исследований необходимо выявлять основные враждебные группы и постоянно изучать и отслеживать их деятельность. Таким образом, ключевым моментом является возможность простого в использовании и узконаправленного анализа!

- **Эффективные шаги по борьбе с использованием террористами Интернета требуют сильных и взаимовыгодных государственно-частных партнерств (ГЧП)**. Государства не меньше бизнеса заинтересованы в безопасном киберпространстве как элемента защиты их финансовых интересов и репутации. Необходимо запрашивать и систематически использовать опыт и технические знания, которыми владеет частный сектор, в том числе путем формулирования четких, понятных законов, регулирующих сотрудничество с учетом роли и обязанностей каждой из сторон. Такое сотрудничество также может основываться на рекомендациях по сотрудничеству, вырабатываемых совместно и реализуемых всеми заинтересованными сторонами, выразившими однозначную готовность к долгосрочной работе. В рамках эффективного сотрудничества обе стороны должны определить контактных лиц, наделенных правами и возможностями выступать от имени своей стороны. В этом отношении сотрудничество с частным сектором может быть также усилено, например, путем создания организационной структуры, позволяющей частному сектору выступать от одного лица. Необходимо продолжить обсуждение вопроса об ответственности компаний или самого пользователя в связи с неадекватными мерами кибербезопасности или безопасности информационно-коммуникационных технологий. *Существующие ГЧП, или вклады частного сектора, необходимо поддерживать, например, механизмами маркировки и передачи информации либо с помощью передовой практики сотрудничества, и в этом отношении такие организации как ОБСЕ могут стать ключевыми сторонами, поддерживающими такие усилия и инициативы государственного образования*.

- **Интернет-пользователи являются важной частью борьбы с использованием террористами Интернета.** На индивидуальном уровне существует потребность в повышении осведомленности конечного пользователя об ответственном использовании Интернета и о возможных последствиях неосторожного раскрытия личных данных. Повышение осведомленности и обучение отдельных интернет-пользователей тому, как сохранять безопасность, должно начинаться в начале школьного образования, например, путем включения в него экзамена по кибербезопасности и безопасности информационно-коммуникационных систем, и продолжаться в течение всей рабочей карьеры и пенсионного возраста человека. На групповом уровне для интернет-пользователей необходимо создать механизмы и системы, с помощью которых они смогут контролировать друг друга. Сюда необходимо включить соответствующие механизмы передачи информации и маркировки со стороны частного и/или государственного сектора и знания о том, какую информацию необходимо направлять. Организации гражданского общества играют особую роль в этом отношении, как в плане борьбы с идеями террористов, так

и в плане укрепления устойчивости конечного пользователя и сообщения о террористическом контенте в соответствующие органы. Необходимо продолжить обсуждение ответственности пользователя, а также вопроса о том, как привлекать интернет-пользователей к оказанию помощи при возникновении чрезвычайных ситуаций. *ОБСЕ могла бы сыграть ключевую роль в том, чтобы стимулировать государства к внедрению таких образовательных программ и предлагать свои возможности по организации помощи в этом отношении.*

- **Требуется взаимное обогащение усилий, направленных на борьбу с различными формами (насильственного) экстремизма в Интернете.** Несмотря на то, что важно признавать преступления на почве нетерпимости и другие формы правого экстремизма в качестве отдельного вопроса и разбираться с ними на этом основании, особенно с точки зрения образования, повышения осведомленности, реагирования органов правопорядка и судебных органов, все же возникает вопрос возможного дублирования усилий по предотвращению таких выражений насилия и предотвращению терроризма. Например, требуется более подробное исследование переломных моментов, в которые экстремистские взгляды принимают насильственную форму. Это означает, что необходимо опубликовать базовую информацию, которая сможет использоваться для борьбы со всеми формами экстремизма. Такая информация должна включать все факторы, в том числе мотивацию, обеспечивая лучшую подготовку к возможным новым формам насильственного экстремизма в будущем. В этом отношении также важно активизировать усилия по сопоставлению методов и выявлению общих черт между разными формами контрмер для борьбы с разными формами экстремизма, например, борьбы с идеями и борьбы с ксенофобскими высказываниями. *ОБСЕ со своим комплексным подходом к безопасности могла бы возглавить сбалансированный анализ путем рассмотрения указанных выше вопросов.*

III. История вопроса

Мандат и деятельность ДПТУ/АТП

Обеспокоенные масштабами использования Интернета террористическими организациями, государства-участники ОБСЕ приняли два Решения Совета министров, которые служат основой постоянной роли ДПТУ/АТП в этой области. В частности, государства-участники приняли на себя обязательства по обмену информацией об использовании Интернета в террористических целях и определению возможных стратегий борьбы с этой угрозой, обеспечивая в тоже время соблюдение международных обязательств и норм в области прав человека (MC.DEC/3/04). Они также решили, помимо прочего, активизировать свою деятельность путем укрепления международного сотрудничества в деле противодействия использованию Интернета для террористических целей […] и изучить возможность более активного вовлечения институтов гражданского общества и частного сектора в деятельность по предупреждению и борьбы против использования Интернета для террористических целей (MC.DEC/7/06).

Недавно государства-участники приняли Решение Постоянного совета № 1063 «Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом» (декабрь 2012 г.). В Консолидированной концептуальной базе, помимо прочего, противодействие использованию Интернета в террористических целях признается стратегическим направлением контртеррористической деятельности ОБСЕ, в соответствии с принятыми контртеррористическими обязательствами и существующими мандатами ОБСЕ. Кроме того, сравнительным преимуществом в области антитеррористической деятельности признается комплексный подход ОБСЕ к вопросам безопасности, а также структура этой организации, позволяющая вести диалог заинтересованных сторон, повышать осведомленность, обмениваться знаниями и опытом, передовой практикой и извлеченными уроками.

ДПТУ/АТП оказывало содействие государствам-участникам ОБСЕ в исполнении их обязательств в области противодействия использованию террористами Интернета, организовав с 2005 года четыре мероприятия в рамках всей ОБСЕ, а также три национальных семинара. Сравнительное преимущество усилий ОБСЕ в сфере использования террористами Интернета заключается в том, что они встроены в более широкие усилия этой организации по продвижению всеобъемлющего подхода к кибербезопасности и безопасности информационно-коммуникационных технологий. Это позволяет рассматривать определенную группу нарушителей на основе межизмеренческого и интегрированного подхода, признающего взаимосвязи киберугроз и нарушителей, и подчеркивает необходимость реакции с учетом соблюдения прав человека. На практике эта гибкость позволяет ДПТУ/АТП мыслить нестандартно, использовать собственные наработки и предлагать комплексную платформу для формирования информации по данной теме, предлагая принимающим странам возможность проверить их собственные усилия по кибербезопасности и безопасности информационно-коммуникационных технологий и выявить несоответствия.

Онлайн-форумы 2012 г.

Дискуссии на экспертных онлайн-форумах 2012 г. были призваны укрепить и стимулировать информационный обмен о последних тенденциях и спорах в отношении использования террористами Интернета и пролить свет на онлайн-деятельность террористов и их мотивы. Онлайн-форумы были посвящены четырем темам: 1. Использование Интернета террористами как тактического средства (21-25 мая 2012 г.); 2. Использование террористами инструментов социальных сетей (2-6 июля 2012 г.); 3. Использование Интернета правыми экстремистами и террористами (17-21 сентября 2012 г.); и 4. Эффективные государственно-частные партнерства для противодействия использования Интернета террористами (8-12 октября 2012 г.).

Дискуссии на каждом форуме были основаны на материалах для обсуждения, подготовленных ДПТУ/АТП и предоставленных государствам-участникам до начала форумов. В настоящем отчете они использовались в качестве вступлений к описаниям различных направлений обсуждения на форумах. Материалы для обсуждения были разработаны в тесном сотрудничестве с другими важными исполнительными структурами ОБСЕ, такими как Бюро ОБСЕ по демократическим институтам и правам человека и Представитель ОБСЕ по вопросам свободы СМИ. Кроме того, группа экспертов с

международным признанием и активных участников деятельности ОБСЕ в этой области выступила с предложением рассмотреть материалы для обсуждения, а также внести значительный вклад в дискуссии, проводимые на форумах, в том числе в роли «инициаторов» и «участников дискуссий» (см. Приложение А). Модераторами во время самих обсуждений выступали ответственный сотрудник ДПТУ/АТП по вопросам, относящимся к противодействию использования Интернета в террористических целях, и специалист по кибербезопасности Департамента по противодействию транснациональным угрозам.

IV. Межотраслевые вопросы: права человека

Во время обсуждений ведущим являлся принцип, что любые дебаты по вопросам и ответам в связи со сложными задачами, вытекающими из использования террористами Интернета, необходимо закреплять в обязательствах государств-участников ОБСЕ по защите прав человека, в частности, права на неприкосновенность частной жизни (включая защиту данных), свободы вероисповедания и убеждений и свободу выражения мнения, закрепленных в нескольких согласованных документах ОБСЕ[2], включая обязательства, имеющие политическую силу.

Государства-участники ОБСЕ неоднократно признавали важнейшую связь между эффективными стратегиями противодействия терроризму и соблюдением прав человека, и также то, что контртеррористические меры, не защищающие права человека, являются контрпродуктивными. Они приняли на себя обязательства по предотвращению и борьбе против терроризма в полном соответствии с международными стандартами прав человека.

Неотъемлемой частью такого подхода является то, что радикализация и экстремизм не должны быть целью контртеррористических мер органов правопорядка, если они не связаны с насилием или иными неправомерными действиями, юридические определения которых соответствуют международному законодательству о правах человека (например, когда группы, считающиеся радикальными или экстремистскими, не прибегают к преступным действиям и/или насилию, не подстрекают к ним и не оправдывают их). Исповедование взглядов или убеждений, которые считаются радикальными или экстремистскими, а также их мирное выражение само по себе не должно считаться преступлением.

На форумах было вновь подчеркнуто, что в Интернете необходимо найти тонкую грань между безопасностью и основными свободами, при этом меры безопасности должны быть временными по своей природе, решение об их применении всегда должно приниматься независимым судом, они должны быть узко направлены на достижение четко поставленной цели, предписаны законом и не должны ограничивать законную речь или использоваться для наложения обязательства по мониторингу.

[2] Обзор соответствующих обязательств представлен на стр. 7 http://www.osce.org/fom/80723

Форум I: Использование Интернета террористами как тактического средства

Мобильные устройства, геолокационные сервисы, электронные финансовые операции и платформы социальных сетей могут привести к практически всеобщей ситуационной осведомленности. Террористические атаки в Мумбаи в 2008 году показали, как террористы используют коммерческие продукты информационных технологий (ИТ) при подготовке и осуществлении своих атак. Интернет оказывает огромное положительное воздействие на мировое население, но в то же время технически грамотные террористы находят пути использования усовершенствованных коммерческих технологий, чтобы получить недорогие версии систем командования, контроля, коммуникаций, расчетов и разведки, ранее доступные только суверенным государствам. На форуме рассматривался вопрос о том, как террористы могут использовать Интернет при планировании и осуществлении своих атак, с обсуждением соответствующих решений. Дискуссии во время форума были посвящены четырем основным темам: 1.) Баланс между потребностями охраны правопорядка и основными свободами; 2.) Освобождение разведывательной информации от излишней детализации и нехватка кадров для сбора данных, дающих основания для действий, 3.) Эффективное привлечение интернет-пользователей к оказанию поддержки; и 4.) Влияние Интернета на будущую террористическую деятельность. [3]

История вопроса

Террористические атаки в Мумбаи в 2008 году, в результате которых погибло 164 человека, показали, что Интернет сыграл важнейшую роль на этапе планирования и во время осуществления этих атак. На этапе планирования террористы провели виртуальную разведку объектов с помощью сетевой картографической службы, что позволило им очень точно организовать выполнение задачи, включая определение входов и выходов, которые должны были использоваться на основных объектах атак, и выяснение географических координат объектов, которые были введены в программы устройств GPS.[4]

В процессе самой атаки террористы использовали свои телефоны Blackberry для передачи информации исполнителям, а также для получения инструкций и новой информации от них, например, данных о местоположении заложников, о международной реакции на атаки и о действиях полиции[5]. Сами исполнители использовали каналы VoIP для того, чтобы скрыть свое физическое местоположение. Уровень тактических деталей, о которых становилось известно из социальных сетей, таких как Twitter или Flickr, мгновенно обеспечивал террористам дополнительную ситуационную осведомленность. Опасаясь, что такая информация может помочь террористам, индийские власти даже сами опубликовали твит с просьбой немедленно прекратить публикацию прямых сообщений в Twitter о событиях в Мумбаи.[6]

[3] Участниками дискуссии на этом форуме были:
[4] http://apdforum.com/en_GB/article/rmiap/articles/print/features/2011/04/01/feature-01
[5] Там же.
[6] http://news.bbc.co.uk/2/hi/south_asia/7752003.stm

С другой стороны, Интернет оказался важнейшим источником информации, особенно для жертв этих атак, которые прятались в гостиницах. Информация в режиме реального времени об атаках, передававшаяся через социальные сети, дала картину того, что там происходило, и стала одним из немногих источников информации для заложников, захваченных террористами.[7] Сама по себе блокада стала экспериментом социальных сетей, поскольку и террористы, и их жертвы, и население Индии и других стран использовали Интернет и мобильные устройства для сбора максимальных объемов информации. Этот эксперимент показал, что ежедневно используемые технологии могут стать основой для осуществления террористических атак, но также продемонстрировал, что доступ к Интернету исключительно важен для сбора информации и обмена ею, как средство связи между гражданами, а в моменты кризиса может даже спасти чьи-то жизни.[8] Однако атаки в Мумбаи и использование террористами Интернета как тактического инструмента также поставили серьезные вопросы перед правоохранительными службами о том, как действовать в отношении этого нового компонента террористических атак.

Сложные задачи

Сбор разведывательных данных

Террористы, подобные организаторам терактов в Мумбаи, могут анализировать данные, поступающие из разных источников, и способны сводить их к полезной тактической информации. Такая информация может поступать как из открытых источников, например, из сервисов схем расположения или туристических сайтов, так и с сайтов социальных сетей, защищенных паролями. Суть в том, что террористы собирают, казалось бы, безобидную информацию из многочисленных источников, в результате получая полную картину, дающую им тактическую ситуационную осведомленность. Признавая вероятность злоупотребления на первый взгляд незначительной личной информацией, американская армия недавно предупредила военнослужащих об опасности «геомаркировки». В частности, армейские руководители указали, что смартфоны имеют встроенные устройства GPS, а на сделанных с их помощью фотографиях автоматически выставляются показатели широты и долготы места, где они были сняты – и эта информация может дать преимущества террористам, обладающим необходимым программным обеспечением.[9] Аналогичным образом, платформы социальных сетей теперь дают пользователям возможность указывать их местоположение при публикации сообщений. В сочетании с последней информацией о ежедневных действиях человека и часто небрежным отношением многих пользователей социальных сетей к принятию «друзей» или к раскрытию собственных частных данных, платформы социальных сетей потенциально дают террористам возможность эксплуатировать интернет-пользователей для собственной выгоды. Предварительное изучение открытых источников создает сложности для правоохранительных органов, поскольку эти виды террористической деятельности вряд ли можно контролировать. Таким образом, соответствующие предупредительные, эффективные контрмеры, предусматривающие соблюдение прав

[7] http://www.ngonlinenews.com/news/mumbai-attacks-and-social-media/
[8] Там же.
[9] http://www.army.mil/article/75165/Geotagging_poses_security_risks/

человека, вероятно, потребуют сотрудничества с общественностью, что было признано в качестве практики во многих странах, а также с частными поставщиками онлайн-услуг.[10]

Стратегическая/тактическая коммуникация

Новые технологии и формы коммуникации в сети и способы получения доступа к ней, включая Протокол передачи голоса через Интернет (VoIP), форумы социальных сетей, виртуальные миры и ведение микро-блогов означают огромные объемы коммуникационных данных и потенциально дают возможность террористам маскироваться и прятать тактические связи за «шумом».[11] Например, с помощью традиционных методов условного отслеживания правоохранительные органы могут проследить звонки с наземной линии связи или мобильного телефона подписчику VoIP лишь до этапа коммутационной станции, преобразующей голосовой звонок в интернет-данные.[12] Кроме того, хотя во многих странах поставщики информационных услуг (ПИУ) обязаны хранить интернет-данные в течение определенного периода времени, эти правила нечасто применяются к записям VoIP. Помимо этого, террористы могут использовать методы шифрования данных, многократного шифрования и сокрытия факта передачи сообщений, доступные на рынке либо создаваемые террористами для террористов.[13] Также существуют свидетельства того, что террористы все больше используют систему персональной сети Bluetooth для трансляции на локализованной основе между определенными пользователями – такую связь правоохранительные органы и спецслужбы выявить не могут.[14] Большое число каналов связи, как зашифрованных, так и открытых, может испытывать возможности правоохранительных органов, которые сталкиваются с проблемой ограниченных ресурсов. Несмотря на то, что власти могут собирать большие объемы данных, перехват и расшифровка коммуникационных данных террористов при условии соблюдения прав человека требуют значительных технических знаний и большого количества подготовленных специалистов для получения ценной оперативной информации.

Диверсификация доступа к Интернету и хранение данных

Смартфоны и возможность приобретать незарегистрированные SIM-карты во многих странах позволяют террористам использовать Интернет, избегая каких-либо форм идентификации личности.[15] К тому же благодаря небольшим размерам смартфонов, их легко украсть и выбросить после достижения необходимой цели, что еще больше затрудняет работу правоохранительных органов по отслеживанию онлайн-деятельности определенного лица. Более того, облачные вычисления позволяют террористам хранить цифровой контент в юрисдикциях, не склонных к международному сотрудничеству, не опасаясь, таким образом, опознания.[16] Сами по себе облачные вычисления представляют еще одну мало изученную область в плане международного сотрудничества

[10] Например, Великобритания создала Справочное бюро по Интернету, отслеживающее жалобы публики на подозрения о деятельности террористов в Интернете.
[11] http://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf
[12] http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html
[13] http://www.reuters.com/article/2008/01/18/us-internet-islamists-software-idUSL1885793320080118
[14] http://eandt.theiet.org/magazine/2011/07/terrorisms-invisible-propaganda.cfm
[15] http://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf
[16] Там же.

правоохранительных органов и ответственности юрисдикции. Эксперты также указали, среди прочего, и на другую методику, а именно, хостинг на быстрых нейтронах, представляющий собой метод постоянного перемещения местоположения веб-сайта, электронной почты или системы доменных имен от компьютера к компьютеру, который потенциально также может использоваться террористами.[17] Что касается ответных мер, то диверсификация мобильных устройств и возможностей хранения информации значительно осложняет расследования, ведущиеся правоохранительными органами и криминалистами. Дело не только в относительной новизне приложений и наборов инструментов по криминалистике для мобильных устройств, но и в том, что их разработчикам также сложно успевать за новыми технологическими достижениями.[18] В целом темпы их разработки также напрямую связаны с потребностями в обучении персонала правоохранительных органов, судебных органов, а также политиков.

Установление подлинности, анонимность и потребность в надежных формах идентификации

Широкое использование Интернета террористами в Мумбаи при планировании и проведении их атак, которое никто не смог выявить, еще раз показало одно из основных препятствий в борьбе со злонамеренным использованием киберпространства – анонимность, и как следствие – сложную задачу, стоящую перед властями, по связи определенной кибердеятельности с конкретным нарушителем. В кратком руководстве, недавно изданном Целевой группой по осуществлению контртеррористических мероприятий (ЦГОКМ) *«Борьба с использованием Интернета в террористических целях — Правовые и технические вопросы»* отмечено, что требуются более надежные формы идентификации в киберпространстве для того, чтобы можно было оказывать сдерживающее воздействие на использование террористами Интернета.[19] Это замечание особенно важно, поскольку Интернет может дать гражданам права и возможности и потенциально ускорить процессы демократизации, а также позволить гражданам получить доступ к политической, культурной и социальной информации.[20] Этические вопросы, связанные с онлайн-анонимностью, а также время, которое, очевидно, потребуется для того, чтобы найти адекватные технические решения, могут указывать на необходимость установления определенных правил поведения в киберпространстве, дополненных Мерами по укреплению доверия. [21]

[17] http://www.icann.org/en/news/announcements/announcement-26jan09-en.htm
[18] http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/
[19] http://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf
[20] http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=685672482
[21] См., например, соответствующую работу ОБСЕ и Решение Постоянного совета № 1038 «О разработке мер по укреплению доверия для снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий».

Краткое описание дискуссии

Направление 1: Баланс между потребностями охраны правопорядка и основными свободами

Большие объемы коммуникационных данных указывают на то, что меры правоохранительных органов, направленные на противодействие использованию террористами Интернета как тактического средства, должны быть скорее упреждающими, чем ответными. Они не должны применяться за счет нарушения прав человека и основных свобод.

- Эксперты подчеркнули, что предотвращение использования террористами Интернета как тактического средства происходит одновременно с возникновением перед правоохранительными и антитеррористическими органами сложных задач. Нарушители могут использовать анонимные коммуникационные технологии или публичные точки доступа к Интернету (например, интернет-кафе), чтобы скрыть свою личность. Кроме того, они могут использовать криптографические технологии для того, чтобы помешать доступу к контенту сообщения, а также к хранящимся данным. В связи с этой анонимностью некоторые страны ввели инструменты интенсивного расследования, например, Раздел 49 Закона о правах следственных органов Великобритании 2000 г. (RIPA) обязывает подозреваемого предоставить пароли к зашифрованному материалу. Разные юрисдикции пришли к разным выводам в отношении того, как это повлияло на основные права человека, особенно в отношении запрета свидетельствования против самого себя. Кроме того, законы, обязывающие подозреваемых выдавать ключи к зашифрованному материалу, часто не учитывают такие новые технологии как Truecrypt, которые позволяют скрывать контент даже при выдаче паролей.

- Несмотря на то, что контролировать весь сетевой контент террористического и криминального характера невозможно, и эксперты подчеркивают, что лучше сохранить открытый Интернет и собирать свидетельства для преследования нарушителей, чем закрывать сайты, иногда принудительные меры неизбежны, особенно, если действия пользователей выходят за определенные границы, например, в случае подстрекательства к насилию или возникновения непосредственной угрозы. Однако такие меры, включающие блокирование веб-сайтов или удаление материалов, которые часто вызывают противоречивое отношение публики, должны приниматься в соответствии с четко сформулированными национальными законами и принципами, соблюдающими основные права и устанавливающими какими угрозами оправдываются конкретные меры. Кроме того, важно создать эффективную систему надзора, при которой пострадавшая сторона будет иметь возможность подать жалобу в случае применения к ней неправомерных санкций. В разработку политики, связанной с принудительными мерами, необходимо вовлекать общественность и гражданское общество и обращаться к ним за содействием. Это важно для того, чтобы объяснить, чего пытаются добиться власти, и чтобы избежать отрицательной реакции общественности, которая, в свою очередь, создает возможности для

развития терроризма. Аналогичным образом, власти должны принимать во внимание то, как такие усилия повлияют на международное сотрудничество.

- Несмотря на то, что эксперты в целом соглашаются с важностью принудительных мер для борьбы с онлайн-деятельностью террористов, если она угрожает национальной безопасности, принятие соответствующих мер на международном уровне оказывается более сложной задачей, либо такие меры могут потенциально ухудшить ситуацию в отсутствие гармонизированной международной правовой системы. Например, ответные меры правоохранительных органов на действия веб-сайтов с хостингом в третьей стране могут не только восприниматься как атака на национальную инфраструктуру, но и воспрепятствовать ведущемуся полицейскому расследованию. Кроме того, то, что одна страна считает приемлемой ответной мерой на чрезвычайную ситуацию, открывает двери для широкого спектра ответных мер других стран, у которых могут возникнуть другие, хотя также закономерные опасения в отношении контента иного типа.

- Эксперты подчеркнули важность гармонизации международной правовой системы для достижения эффективного международного сотрудничества. Однако это стало бы лишь первым шагом. Скорость и транснациональный характер Интернета постоянно подвергают проверке пределы традиционных видов международного сотрудничества. В частности, один эксперт привел в пример компанию PayPal, которая указала, что только в редких случаях «данные предоставлялись запрашивающим правоохранительным органам в сроки менее трех месяцев. Чаще всего на это уходит шесть месяцев (…), а бывает, что данные предоставляются более чем через два года после того, как они были запрошены. Учитывая скорость, с которой происходят кибератаки, это фактически связывает руки правоохранительным органам и часто наносит урон расследованию».[22] В связи с этим эксперты призывают к установлению более прямых линий связи между правоохранительными органами, а также косвенного сотрудничества через дипломатические миссии для обеспечения своевременной реакции и надлежащих ответных мер террористам, использующим Интернет в качестве тактического средства.

- Эксперты подчеркнули, что международные организации могли бы стать идеальным местом для оценки потенциальных принудительных мер, не только в плане их совместимости с основными свободами, но и в отношении оценки издержек и выгод таких мер.

[22] https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf

Направление 2: Освобождение разведывательной информации от излишней детализации

В периоды бюджетных ограничений специально обученный персонал, способный анализировать постоянно растущие объемы передаваемых данных, должен работать максимально эффективно.

- Эксперты указали, что при сборе разведывательных данных в рамках противодействия киберугрозам необходимо учитывать человеческий фактор. Несмотря на то, что власти способны собирать огромные объемы данных, возникают проблемы с большим количеством информации, поскольку технические возможности целенаправленной тщательной проверки таких данных развиваются не столь быстрыми темпами. Специально обученные кадры, таким образом, становится важнейшим фактором, особенно в чрезвычайных ситуациях, поскольку 1.) для работы с несистематическими разведывательными киберданными требуется высокий уровень профессионализма, технических знаний и аналитических навыков; и 2.) после анализа разведывательных данных необходимо действовать на их основании, в том числе в сотрудничестве с партнерскими органами и странами. Поэтому так важно обеспечить обучение и укрепление потенциала разведывательных кадров в этих областях. Кроме того, эксперты должны быть обучены тому, как наилучшим образом использовать разведку по открытым источникам, в том числе с использованием таких средств как триангуляция и фальсификация «плохой» информации.

- Эксперты также указали, что преимущества государственно-частных партнерств (ГЧП) пока еще недостаточно используются в связи со сбором и совместным использованием разведывательных данных. Для более эффективного использования всего богатства знаний, которыми обладает частный сектор, властям необходимо установить четкую политику, законодательство, механизмы и процедуры сотрудничества. Также для обеих сторон важно создать координационные центры, действующие в качестве единых контактных точек в рамках обеспечения своевременного сотрудничества.

- Эксперты вновь отметили, что уже существуют международные сообщества, позволяющие осуществлять совместное использование разведывательных данных и информации, связанной с киберпреступлениями и использованием Интернета террористами. И все же некоторые эксперты придерживались мнения, что, хотя такие механизмы являются устойчивыми платформами для сотрудничества, их эффективность порой ограничена из-за того, что они связаны с определенными международными правовыми инструментами, в которых участвуют не все государства-участники. Более того, сама природа разведывательных данных и связанных с ними средств защиты иногда препятствует тому, чтобы распространять такие данные в международных масштабах.

Направление 3: Роль интернет-пользователей

Именно частные интернет-пользователи часто бывают самым слабым звеном с точки зрения борьбы с использованием террористами Интернета как тактического средства, например, из-за небрежного обращения со своей личной информацией. Отдельный интернет-пользователь также является ключом к предотвращению онлайн-деятельности террориста, которая может привести к потенциальным атакам.

- Эксперты подчеркнули, что прежде чем рассматривать пользователя в качестве ключевого участника работы по предотвращению использования террористами Интернета как тактического средства, необходимо разъяснить нынешнюю роль и статус пользователей и степень наделения их правами и возможностями. Например, можно возразить, что неразумно ожидать от обычных интернет-пользователей умелого обращения со сложным набором технологических инструментов и программных решений, доступных в настоящее время, управления ими или принятия информированных решений в отношении этих инструментов. В самом деле, многие пользователи полагаются на знания, навыки, профессионализм, правовые и нормативные структуры, технологические ноу-хау и инженерное мастерство широкого спектра посредников, чтобы те разработали четкие однозначные руководства, надежную аппаратуру и программные решения на основании демократических принципов, производящих надежные, заслуживающие доверия и уважаемые продукты, которыми могут пользоваться обычные потребители. С другой стороны, можно возразить, что именно пользователь умело манипулирует технологическими достижениями эры Интернета нечестными способами, например, планирует и осуществляет террористические атаки. Это отражает поведение пользователей, а не сами технологии. Пользователи, таким образом, могут принять на себя обязательства больше узнать о принадлежащих им инструментах, чтобы понять, что может случиться, и предпринимать разумные меры для защиты своих систем от атак и предотвращать их захват для последующих атак против других людей. Возможно, пользователям необходимо понимать приемлемое использование этой технологии в каждодневной жизни общества и осознавать, что незаконное поведение имеет свои последствия.

- Основной темой обсуждения был вопрос ответственности пользователя. В этой связи основные дебаты развернулись вокруг целесообразности a) разработки своего рода сетевых «водительских прав» и b) возможности реализовать это на практике. Эксперты подчеркнули, что хотя пользователи не знают, как работает их машина, они все равно получают водительские права, поскольку во время экзамена подтверждают понимание правил дорожного движения и возможностей автомобиля, понимают, что машине требуется регулярное техническое обслуживание, знают, как отремонтировать автомобиль и принимают на себя ответственность за заправку машины топливом, замены колес в зависимости от времени года и сообщение об аварии или краже своего автомобиля. Хотя эксперты подчеркивали, что нечто подобное было бы желательно для использования Интернета и защиты компьютеров, они также указали на значительные сложности,

которые возникли бы в связи с этим, поскольку надо будет определить, кто отвечает за сертификацию поведения в сети, как привести такую систему в действие на национальном и международном уровне и с технической, и с административной точки зрения, и как штрафовать за неправильное поведение. Кроме того, возникают вопросы в отношении того, действительно ли властям стоит препятствовать использованию людьми Интернета, и какое воздействие это может оказать на свободу самовыражения и другие основные права.

- Эксперты согласились в том, что киберобразование жизненно необходимо. Повышение осведомленности и образование отдельных интернет-пользователей по вопросам того, как сохранять сетевую безопасность на протяжении всей жизни человека, крайне важно. Это может превратить интернет-пользователей в самое сильное звено с точки зрения кибербезопасности. Такие инициативы должны начинаться в начале школьного образования, например, путем включения в него экзамена по кибербезопасности, и продолжаться в течение всей рабочей карьеры и пенсионного возраста человека. Эксперты предложили, чтобы ОБСЕ играла ключевую роль в том, чтобы стимулировать государства к внедрению таких образовательных программ и предлагать свои возможности по организации помощи в этом отношении. Некоторые эксперты даже предложили, чтобы ОБСЕ оценивала и определяла рейтинг качества национального киберобразования, создавая таким образом стимулы для увеличения инвестиций в эту сферу в странах с более низким качеством образования. В качестве первого шага ОБСЕ могла бы рассмотреть распространение национальной школьной программы киберобразования.

- Эксперты подчеркнули, что частный сектор также мог бы способствовать стимулированию ответственного сетевого поведения интернет-пользователей. Например, многие онлайн-форумы уже разработали методы поддержки и стимулирования хорошего поведения и наказания за плохое поведение. Это часто делается через своего рода систему награждения баллами или значками либо путем предоставления пользователям ряда «званий» или «звезд» в качестве публичного признания их вклада в правильное поведение людей на форуме. Такие механизмы можно было бы распространить шире.

- Эксперты также обсудили потенциальную роль пользователей в выявлении террористов и террористической деятельности в сети. В этом отношении они обсудили «добавленную стоимость» краудсорсинга[23], особенно в условиях чрезвычайных ситуаций. Например, в будущем необходимо рассмотреть, как краудсорсинг используется для выявления лиц, подозреваемых в терроризме, непосредственно после или до неминуемой атаки, помогая правоохранительным органам найти подозреваемых или предотвратить атаку. Однако были озвучены некоторые сомнения в отношении эффективности выявления и сообщения о деятельности террористов в сети пользователями. Например, граждане не всегда

[23] Краудсорсинг представляет собой процесс, предполагающий передачу определенных задач большой группе людей. Этот процесс может происходить как в сети, так и за ее пределами. [1] Краудсорсинг отличается от обычного аутсорсинга, поскольку в данном случае задача или проблема передается неопределенной публике, а не конкретному лицу http://en.wikipedia.org/wiki/Crowdsourcing#cite_note-howedefinition-3

могут делать различия между террористической деятельностью или, например, экстремистскими взглядами. Таким образом, если такая помощь будет привлекаться, подобные жалобы нужно будет направлять не напрямую полиции, а какому-либо «посреднику» (физическому лицу или организации), обладающему необходимыми знаниями и опытом для того, чтобы сортировать и приоритизировать поступающие сообщения.

Направление 4: Воздействие Интернета на будущее терроризма

Интернет и постоянно растущее число инструментов доступа к нему дали террористам потенциальное тактическое преимущество, невиданное никогда ранее до существования Интернета. Вопрос заключается в том, как технологические достижения повлияют на будущее терроризма.

- Эксперты согласились, что новые изменения, связанные с Интернетом, обладают потенциалом для дальнейшего усложнения и без того сложной обстановки для спецслужб, правоохранительных органов и лиц, определяющих политический курс в области отслеживания деятельности террористов в киберпространстве. Основное беспокойство вызывает то, какие последствия может иметь резкий рост использования известных коммерческих сервисов социальных сетей, таких как YouTube, Twitter и Facebook, террористическими организациями и их сторонниками; как постоянные компьютерные вторжения «хактивистов», таких как Anonymous и LulzSec, могут влиять на террористов и мотивировать их; какое воздействие могут оказывать такие новые технологии как darknet или P2P filesharing на деятельность террористов; как контрмеры, предпринимаемые правительствами и виртуальными борцами на террористических сайтах, воздействуют на их технологическое развитие.

- Эксперты также обсудили, как распространение технологии социальных сетей может компенсироваться поддержкой противодействия радикализации для более эффективного сдерживания будущей волны вербовки сторонников террористов в сети. Говоря о контрмерах в более широком смысле, эксперты также указали на приспособляемость и готовность киберпреступников к обучению. Повышение их навыков, в свою очередь, оказывает воздействие на уже недостаточные ресурсы правоохранительных органов. В связи с этим эксперты также указали, что террористы уже обращаются к другим киберпреступникам с целью развития собственных навыков, и эта тенденция, вероятно, сохранится и в будущем. Например, в июне 2011 года Фонд СМИ «Аль-Каиды» Ас-Сахаб выпустил видеоролик под названием «Вы отвечаете только за себя». В этом видео Ас-Сахаб посвятил большой фрагмент теме «электронного джихада», подчеркнув, что те люди, у которых есть навыки хакеров, должны их использовать. Кроме того, директор ФБР Роберт Мюллер сказал, что террористы проявляют явный интерес к приобретению хакерских навыков, и что они предпочитают обучать своих собственных сторонников, чем нанимать чужих, планируя при этом сочетать

физические и кибератаки.[24] В этом отношении все более важную роль для террористов может играть черный рынок. Например, недавняя статья в Forbes показала, что «эксплойты нулевого дня» уже продаются по цене от 5 000 до 250 000 долларов.[25]

- Эксперты указали, что отсутствие гармонизированной правовой системы может усугубить существующие сложности, связанные с международным сотрудничеством; такой же эффект имеет дифференцированное толкование определения пределов наложения оправданных, пропорциональных ограничений, основанных на нормах права и необходимых в демократическом обществе. В этой связи один эксперт отметил, что даже в случае принятия соответствующих законов, в силу природы Интернета это приведет к бесконечной игре в «кошки-мышки» по отслеживанию подобного контента. При этом тот же эксперт подчеркнул, что очевидной границей дозволенного должны быть призывы к насилию или контент, грубо противоречащий всеобщим ценностям человеческого достоинства. В долгосрочной перспективе более эффективная стратегия борьбы с подстрекательством к терроризму могла бы свестись к более «позитивному» использованию Интернета путем противопоставления ненавистнических идей положительным в равном количестве и качестве. Здесь важную роль должны сыграть власти, хотя скорее в роли двигателя, стимулирующего гражданское общество к выходу на «линию фронта». Широта охвата и высокая степень доверия, требуемые для эффективного обращения к людям, обусловливают необходимость государственно-частных партнерств.

[24] http://www.fbi.gov/news/testimony/fbi-budget-for-fiscal-year-2012
[25] http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

Форум II: Использование террористами инструментов социальных сетей

Недавно появились сообщения, что 90% террористической деятельности в Интернете осуществляется с помощью инструментов социальных сетей.[26] То, что террористы используют Интернет, не новость; но то, что почти вся их деятельность ведется в условиях относительной открытости социальных сетей – довольно новая информация. Похоже, террористы превратили дешевые и легкодоступные социальные сети в стратегическое средство для коммуникации, поддержания связей, подстрекательств, восхваления и планирования. Сами по себе социальные сети потенциально могут действовать как фактор повышения боевой эффективности, увеличивающий организационные способности террористической группы, ее возможности по формированию общественных идей, а также как средство привлечения внимания потенциальных сторонников.[27] Форум попытался найти ответы в отношении возможных ответных мер правоохранительных органов, роли интернет-пользователей в ответных мерах на эту угрозу, а также роли частного сектора.

История вопроса

Использование инструментов социальных сетей

Традиционно сетевой контент террористического характера был однонаправленным и основанным на текстах, и существовал либо в форме веб-сайтов, либо в форме текстов и сообщений, размещаемых на форумах. С другой стороны, инструменты и платформы социальных сетей, включая разделы чата, сайты социальных сетей, блоги, сайты для распространения видеоматериалов, позволяют террористам брать на себя больше инициативы.[28] Инструменты социальных сетей могут использоваться террористами для следующих целей:

- **Вербовка и подстрекательство**: вместо того чтобы ждать, когда их потенциальные сторонники зайдут на сайт, содержащий террористическую пропаганду, найдя его благодаря слухам, теперь террористы напрямую обращаются к потенциальным сторонникам или завлекают людей на свои сайты через платформы социальных сетей. Как таковые эти платформы дают террористам дополнительную защиту и возможность «проверить» потенциальных новобранцев. Аналогичным образом, инструменты социальных сетей могут использоваться «заинтересованными» лицами для того, чтобы скрыть свою личность, например, выступая под чужим именем при обращении к террористам. После установления эмоциональной, психологической или интеллектуальной связи между террористом и

[26] Вейманн, Габриэль, 2011 г. *Al Qaeda Has Sent You A Friend Request: («Аль-Каида» отправила вам запрос на включение в список друзей:) Terrorists Using Online Social Networking (как террористы используют социальные сети).*

[27] http://soufangroup.com/news/details/?Article_Id=272

[28] Вейманн, Габриэль, 2011 г. Al Qaeda Has Sent You A Friend Request: («Аль-Каида» отправила вам запрос на включение в список друзей:) Terrorists Using Online Social Networking (как террористы используют социальные сети).

потенциальным террористом, последнему может быть открыт доступ к более скрытому сетевому контенту и материалам.[29]

- **Планирование и стратегические переговоры:** террористы способны анализировать данные из разных источников и объединять их в полезную тактическую информацию для планирования потенциальных атак или для использования во время активных террористических кампаний. Например, потенциально они могут воспользоваться неосторожным раскрытием личных данных интернет-пользователей на сайтах социальных сетей, включая информацию о ежедневной деятельности человека, его сообщения с указанием местонахождения и фотографиями, используя свойственное порой пользователям социальных сетей небрежное отношение к положительным ответам на включение незнакомых людей в «друзья». Более того, как показали террористические атаки 2008 года в Мумбаи, уровень тактических деталей, о которых становилось известно из социальных сетей, таких как Twitter или Flickr, может дать террористам мгновенную ситуационную осведомленность в обход таких традиционных контрмер, принимаемых правоохранительными органами, как блокирование мобильных телефонов.

- **Обращение к публике и восхваление:** террористы научились использовать платформы социальных сетей для пропаганды своих идей и формирования общественного мнения до или вскоре после атак. У таких террористических организаций, как «Аль-Каида», есть собственные пресс-службы, и атаки часто снимаются и распространяются в сети спустя лишь несколько мнгновений после их осуществления.[30] Они предлагают свою версию реальности, часто прославляя насилие и то, что они считают успехом. Такая деятельность, в свою очередь, потенциально усиливает общественные страхи и может произвести впечатление на людей, придерживающихся аналогичных взглядов, что нередко дает и тактическое, и стратегическое преимущество террористам и в их террористической операции, и в целом для их целей.

Инструменты социальных сетей

Инструменты сетей, которыми могут злоупотреблять террористы, включают:

- **Тематические чаты:** тематические чаты позволяют не только «жителям» Интернета, НГО, организациям гражданского общества, но и террористическим группам общаться с единомышленниками и сторонниками по всему миру, вербовать новых последователей и делиться информацией, почти не подвергаясь риску разоблачения властями. Например, среди террористов стал особенно популярен открытый сервис тематических чатов PalTalk, который включает голосовые и видеовозможности.[31] Помимо цели получения поддержки,

[29] Там же.
[30] Например, см. http://www.npr.org/templates/story/story.php?storyId=5548044
[31] Вейманн, Габриэль, 2011 г. *Al Qaeda Has Sent You A Friend Request: («Аль-Каида» отправила вам запрос на включение в список друзей:) Terrorists Using Online Social Networking (как террористы используют социальные сети).*

тематические чаты также служат для распространения тактической информации среди «экспертов», поскольку в них даются прямые ответы на такие вопросы, как собрать бомбу или как взломать компьютерную систему.

- **Блоги:** в докладе, подготовленном 304 батальоном военной разведки армии США, подчеркивается, что такие блог-сервисы как Twitter могут стать для террористов эффективным инструментом координации атак – что было продемонстрировано во время атак 2008 года в Мумбаи. В отчете также говорится о возможных сценариях использования террористами этого онлайн-формата, включая получение информации о местоположении потенциальных объектов атаки практически в режиме реального времени, или, например, взлом страницы солдата и общение с другими солдатами от его имени.[32]

- **Сайты социальных сетей**: виртуальные сообщества становятся все популярнее, особенно среди молодежи. Веб-сайты социальных сетей позволяют террористам обращаться к восприимчивой возрастной группе, которая может сочувствовать их идеям. Кроме того, многие пользователи социальных сетей неосторожно принимают запросы на включение в список «друзей», что может дать террористам возможность получить доступ к их личной информации. Также существуют различные террористические группы, имеющие открытые страницы на сайтах социальных сетей, где любой интересующийся может ознакомиться с размещенной там информацией, почитать дискуссии, посмотреть пропагандистские видеоролики и вступить в такую группу.[33]

- **Распространение видеоматериалов:** террористы используют сетевые платформы,[34] на которых размещаются и распространяются видеоматериалы, и осужденные террористы открыто говорят об их пользе для привлечения средств, разжигания ненависти и пропаганды.[35] Помимо этого, в результате исследования, посвященного высказываниям и комментариям по поводу сетевых видеоматериалов, было установлено, что сетевые видеоматериалы получают глобальную аудиторию, особенно среди молодых зрителей, и такой террористический контент распространяется далеко за пределы своей предполагаемой основной базы поддержки.[36]

---

[32] http://afp.google.com/article/ALeqM5jGd91R-NdcJLa8N6OBU76hbrVFyg

[33] Вейманн, Габриэль, 2011 г. *Al Qaeda Has Sent You A Friend Request: («Аль-Каида» отправила вам запрос на включение в список друзей:) Terrorists Using Online Social Networking (как террористы используют социальные сети).*

[34] Например, http://news.sky.com/home/uk-news/article/15210314

[35] http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3547072/JihadistforumJihadist--calls-for-YouTube-Invasion.html

[36] Конвей, Маура и Лиза МакИнерни, 2008 г. "Jihadi Video & Auto-Radicalisation: («Джихад-видео и саморадикализация:) Evidence from an Exploratory YouTube Study" (результаты исследования YouTube). В *Тезисах 1-ой Европейской конференции о разведывательной информации и безопасности,* Эсбьерг, Дания, 3-5 декабря 2008 г.

Краткое описание дискуссии

Направление 1: Улучшение реакции правоохранительных органов

Учитывая бюджетные ограничения, специально обученные кадры, способные анализировать и реагировать на использование террористами инструментов социальных сетей, должны работать максимально эффективно.

- Эксперты подчеркивают, что форумы для общения и социальные сети все больше демонстрируют и свои преимущества, и недостатки. В то время как террористы используют их потенциал для коммуникации, налаживания отношений, подстрекательства, восхваления и операционного планирования, правоохранительные органы также могут привлекать эти инструменты для получения более глубокого представления о деятельности террористов, собирая при этом свидетельства для преследования виновников преступной деятельности. Эксперты подчеркнули, что принимаемые ответные меры в первую очередь должны учитывать соответствующие правовые процедуры, защиту данных, дискриминацию, неприкосновенность частной жизни и вопросы, связанные с профилированием, в сочетании с обеспечением гарантии свободы мнений и выражения и права на свободу собраний.

- Учитывая ценность информации, размещаемой на сайтах социальных сетей, аналитики правоохранительных органов по всему миру уже изучают информацию, размещаемую в Twitter и Facebook, для сбора разведывательных данных в рамках борьбы с использованием террористами сайтов социальных сетей, что представляет собой очень трудоемкую работу. Поскольку им приходится иметь дело с огромными объемами данных, некоторые правоохранительные органы вкладывают средства в развитие цифровых инструментов, способных сканировать весь спектр социальных сетей, что позволяет получать больше данных. Эксперты подчеркнули, что такие технологии крайне важны, если учесть соотношение количества сотрудников правоохранительных органов и киберпреступников, включая террористов.

- Однако существуют и сомнения в пользе таких инструментов: многие эксперты отметили, что основная трудность заключается в том, чтобы научить компьютеры читать. Например, как программа может определить разницу между ценной информацией и тонкими различиями смысла с одной стороны, и «шуткой» с другой. Кроме того, также возникает проблема с аутентичностью, когда речь идет о компьютерных программах, известных как спам-боты, которые уже не дают покоя таким сервисам как Twitter своими «мусорными» сообщениями, аналогичными спаму в электронной почте. Многие эксперты полагают, что возможности создавать спам-ботов только увеличатся со временем, и потенциально они смогут обманывать аналитиков и их программы, которые будут думать, что имеют дело с деятельностью реального человека, в то время как она будет искусственно созданной с целью вводить в заблуждение. Кроме того, применение технологии отслеживания без определения узкой и направленной

правоохранительной цели также вызывает вопросы с точки зрения прав человека и основных свобод, даже если информация общедоступна, а действия не направлены на конкретных групп или определенных лиц. Эксперты также подчеркнули, что в конечном итоге все равно потребуются обученные специалисты, которые будут отсеивать данные, собранные программами или внешними источниками, и принимать соответствующие меры.

- Эксперты спорят о том, что является более эффективным – применение правоохранительными органами предупредительных мер, или применение мер пресечения и реагирования в борьбе с использованием террористами инструментов социальных сетей, о чем часто говорят как о выборе между закрытием сайтов и их использованием. Например, одни эксперты указывают на недавнее исследование Кембриджского университета, в котором делается вывод, что стратегические кампании, нацеленные на криминальные сети, могут на самом деле быть более экономичным инструментом для повышения уровня кибербезопасности. В то же время другие эксперты говорят о международном «правовом минном поле», которое не только затрудняет такие ответные меры, но и создает такую ситуацию, когда принудительные меры могут также отрицательно сказаться на будущем международном сотрудничестве. Таким образом, некоторые эксперты полагают, что важнее сначала рассмотреть возможность гармонизации международной правовой системы и преимущественно придерживаться превентивных мер на рабочем уровне, включая соглашения о совместных расследованиях силами правоохранительных органов, например, в рамках таких организаций как Организация договора коллективной безопасности.

- Эксперты также предположили, что органы охраны правопорядка должны больше полагаться на частный сектор или обдумать более тесные связи с ним, а также приложить соответствующие усилия для противодействия умышленным противоправным действиям. Например, один эксперт указал на подразделение цифровых преступлений компании Microsoft. Это подразделение в настоящее время занимается созданием препятствий для наиболее сложных угроз киберпреступлений, такие как использование технологий для сексуальной эксплуатации детей и умышленные программные преступления, особенно интернет-атаки ботов. Они занимаются этим в тесном сотрудничестве с отраслью, правоохранительными органами, научным сообществом, государственными органами и НГО по всему миру. [37]

[37] http://www.microsoft.com/government/ww/safety-defense/initiatives/pages/digital-crimes-unit.aspx

Направление 2: Наделение интернет-пользователей и гражданского общества правами и возможностями

Социальные сети играют важную роль в предотвращении использования террористами инструментов социальных сетей и борьбе с ним.

- Эксперты подчеркнули, что концепции «последней линии обороны» и «службы экстренного реагирования» представляют собой подходящие отправные точки для рассмотрения роли и прав конечных пользователей в борьбе с использованием террористами инструментов социальных сетей. Можно утверждать, что конечные пользователи сами заинтересованы в безопасных и защищенных социальных сетях. В качестве службы экстренного реагирования, пользователи должны быть в состоянии распознавать случаи злонамеренного использования социальных сетей террористами и иметь стимулы для сообщения о таких случаях операторам социальных сетей, компетентным государственным органам и/или организациям гражданского общества. В качестве «последней линии обороны», отдельные пользователи должны быть обучены ответственному сетевому поведению, разбираться в вопросах конфиденциальности и рисках, связанных с раскрытием личных данных и иной потенциально секретной информации через социальные сети. Индивидуальные пользователи также должны быть устойчивы к распространяемым через социальные сети сообщениям и контенту, имеющим насильственный характер или потенциально являющимся сигналом к насильственному отношению.

- Эксперты подчеркнули особую роль организаций гражданского общества. Организации гражданского общества играют крайне важную роль в укреплении устойчивости конечных пользователей к насильственному контенту и в усилиях по завоеванию «сердец и умов». Важно, что организации гражданского общества основывают свою деятельность на допустимости, надежности и свободе действий, которых может не быть у государственных властей, особенно при борьбе с ненасильственным экстремизмом. Их следует стимулировать к использованию социальных сетей для формулирования и распространения позитивных обращений и контрмер, противостоящих террористической пропаганде и разжиганию вражды.

- Социальные сети дают организациям гражданского общества уникальные инструменты защиты: получение возможности выразить свое несогласие, инновационные способы оформления и целенаправленное обращение к конкретной аудитории. Например, инструменты социальных сетей можно использовать для объединения конечных пользователей и других заинтересованных лиц, таких как бывшие насильственные экстремисты и пострадавшие, в рамках создания интерактивных сообществ на основе позитивных ценностей. Аналогичным образом, организации гражданского общества могут быть задействованы в мониторинге и механизмах предоставления рекомендаций для выявления и рассмотрения подозрительных материалов или действий,

включая организацию «сетевого превентивного вмешательства» для взаимодействия с конечными пользователями, подвергающимися риску.

- Эксперты отметили, что некоторые операторы социальных сетей предлагают механизмы, которые могли бы применять пользователи для маркировки контента, нарушающего правила сообщества или условия обслуживания. Однако пока неясно, насколько часто такие возможности фактически используются, и сколько людей занимается отсевом такого контента. Также неясно, в какой степени компании информируют пользователей о таких возможностях и стимулируют людей к их использованию. Фактически поощрение использования таких механизмов может быть контрпродуктивным и дорогостоящим для операторов и представлять собой репутационный риск. В будущем подобные дебаты необходимо сосредоточить, во-первых, на том, как стимулировать пользователей к применению таких возможностей, а во-вторых, на том, какие стимулы можно было бы создать, чтобы операторы активно продвигали такие системы.

- Эксперты указали, что особую сложность при обучении интернет-пользователей безопасному использованию инструментов социальных сетей представляет собой динамичная среда самого Интернета. Например, Facebook не существовал еще десять лет назад, а Twitter едва исполнилось пять лет. Другая сложность заключается в стимулировании пользователей к фактическому применению их знаний о кибербезопасности. В связи с этим киберобразованию необходимо сосредоточиться как на практических мерах, так и на изменении поведения, т.е. поощрять пользователей к безопасному поведению в течение длительного периода времени. В этом отношении стимулы крайне важны для периодического поощрения хорошего поведения.

Направление 3: Роль частного сектора

Поскольку большинство инструментов социальных сетей принадлежит частным компаниям, прозрачные, институанализированные и взаимовыгодные государственно-частные партнерства исключительно важны для предотвращения злоупотребления террористами инструментов социальных сетей и в интересах поставщиков услуг социальных сетей.

- Эксперты отметили, что предотвращение использования террористами инструментов социальных сетей и борьба с этим явлением преимущественно является обязанностью органов государственной власти. В связи с этим являются необоснованными потенциальные обязательства, налагаемые на операторов социальных сетей, по мониторингу социальных сетей, а также повышение ответственности частного сектора за запрет, закрытие сайтов или уведомление властей. Однако эксперты также указали, что у частного сектора есть коммерческий интерес во внесении своего вклада в эту работу и в поиске взаимоприемлемых решений о сотрудничестве.

- Для того чтобы получить широкомасштабную поддержку частного сектора, было предложено обратиться к корпоративной социальной ответственности операторов социальных сетей и к их интересу к защите собственного имиджа и репутации. Однако при рассмотрении репутационных вопросов власти должны быть осторожны в связи с тем, что владельцы и операторы социальных сетей могут опасаться того, чтобы не выглядеть в глазах пользователей и клиентов агентами или представителями правительства.

- Было отмечено, что многие провайдеры уже приняли разного рода меры по защите своих сетей от террористических материалов, например, путем изъятия видеоматериалов с террористической пропагандой. Однако такие ответные меры были несистематическими, и разными владельцами применялись разные правила. Одна из идей в этом отношении заключалась в том, чтобы разработать добровольные руководящие принципы, которые можно было бы применять повсеместно и которые давали бы определенную степень устойчивости. В этом отношении важно подумать о стимулах для поощрения долгосрочного соблюдения требований (т.е. позитивное закрепление), включая потенциальные (коммерческие) выгоды, например, улучшение репутации, снижение административных затрат или привилегированный доступ к дополнительным ресурсам либо поддержке.

- Эксперты отметили, что многие частные компании уже прилагают усилия по созданию эффективных ГЧП. Однако вклад в такие процессы всегда вносят одни и те же частные компании. В связи с этим эксперты задумались, не стоит ли рассмотреть вопрос о повышении качества не только государственно-частных партнерств, но и частно-частных партнерств. В частности, с точки зрения государственного сектора, вероятно, было бы полезно иметь своего рода организационную структуру или представителя, поддерживаемого большинством частных компаний. Еще одна идея заключалась в том, чтобы частный сектор привлекал на ротационной основе посредников в качестве контактных лиц для государственного сектора, а также международных организаций, стремящихся к обеспечению более высокого качества сотрудничества. Таким образом большинство частных операторов могло бы быть задействовано в этой работе, а затраты потенциально можно было бы разделить между компаниями частного сектора.

Форум III: Использование Интернета правыми экстремистами и террористами: наблюдаемые тенденции и различия

Расследования, в том числе касающиеся недавних резонансных инцидентов в США и Европе, связанных с правым насильственным экстремизмом и терроризмом, показали разнообразную картину уровня угроз, исходящих от подобных лиц и групп, их организационные особенности, а также их согласованность. Например, по данным ЕВРОПОЛ, ультраправый терроризм остается менее значительным, чем другие формы террористической деятельности.[38] С другой стороны, Комитет по внутренним делам Парламента Великобритании пришел к выводу о существовании убедительных доказательств потенциальной угрозы, исходящей от ультраправого терроризма.[39] Отчасти сложности в определении масштабов этой угрозы могут быть связаны с разными способами учета подобных преступлений и противоречивыми концепциями, относящимися к насилию со стороны правых.

Несмотря на это, эксперты соглашаются, что воздействие правого насильственного экстремизма на Интернет должно беспокоить всех.[40] Например, ЕВРОПОЛ заявляет, что Интернет, особенно социальные сети и развитие панъевропейских онлайн-сетей – и то, и другое, оказалось важным в деле Андерса Брейвика – «добавляют новое измерение угрозе правого экстремизма, которая может возникнуть в будущем».[41] Учитывая такие факторы как ухудшение экономической ситуации, более тесная взаимосвязь и согласованность могут ускорить процесс радикализации, который может привести к насилию. Рассмотрение причин, лежащих в основе радикализации, и ответные меры на использование Интернета правыми экстремистами, применяющими насилие, и террористами, таким образом, представляется жизненно важным, независимо от различных оценок уровня угрозы, исходящей от них.

Проблемы, которые обсуждались на форуме, включали вопрос о том, как правые террористы и экстремисты, применяющие насилие, используют Интернет, как это использование отличается от других форм деятельности террористов в Интернете и каковы потенциальные эффективные ответные меры на эту угрозу, в том числе с учетом передовой практики противодействия другим формам насильственного экстремизма в сети.

[38] https://www.europol.europa.eu/sites/default/files/publications/te-sat2011.pdf
[39] http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1446/144610.htm
[40] http://www.iiuedu.eu/press/journals/sds/SDS_2011/DET_Article2.pdf
[41] https://www.europol.europa.eu/sites/default/files/publications/te-sat2011.pdf

Сложные задачи

Правый насильственный экстремизм против терроризма и против преступлений на почве нетерпимости?

При анализе данных по правому терроризму и/или насильственному экстремизму (включая использование Интернета), линия раздела между понятиями иногда представляется размытой. Насильственный экстремизм, преступления на почве нетерпимости и терроризм часто используют как синонимы при описании применения насилия различными лицами в рамках правой идеологии.[42] Например, Институт стратегического диалога в своем недавно изданном документе по результатам проведенной конференции указывает, что «правое насилие по-разному определяется в разных странах Европы, и органы безопасности по-разному учитывают акты насилия»,[43] что затрудняет оценку реальной угрозы и сравнение тенденций. Кроме того, в отчете подчеркивается, что нет ясности и в том, в какой момент группы или лица могут перейти от единичных актов правого экстремистского насилия к планированию террористической деятельности[44], и в отношении того, какую роль играет в этой связи Интернет. Похоже, что мотивами правого насилия, развивающегося из некоторых форм терроризма, насильственного экстремизма и преступлений на почве нетерпимости, могут быть предвзятость и предрассудки людей в рамках правой идеологии. Однако могут существовать либо уже существуют различия в плане интенсивности насилия, целей и предполагаемых объектов, а также адекватных ответных мер. Возможно, ответные меры могут зависеть от того, как государственные власти классифицируют определенное правое насильственное преступление.

Взаимодействие между разными формами насильственного экстремизма и усилия по его предотвращению

Правый насильственный экстремизм преимущественно рассматривался через призму преступлений на почве нетерпимости, в то время как насильственный экстремизм и радикализация «Аль-Каиды» рассматривались через призму терроризма. Вопрос заключается в том, в какой степени превентивные усилия, связанные с предотвращением правого насильственного экстремизма и насильственного экстремизма, вдохновляемого «Аль-Каидой», будут, могут или должны совпадать. Например, Комитет по внутренним делам Парламента Великобритании рекомендовал, чтобы при принятии ответных мер против правого насильственного экстремизма и терроризма признавалось потенциальное взаимодействие между разными формами насильственного экстремизма, и чтобы меры, направленные против правого насильственного экстремизма, оказывали последующее воздействие на другие формы насильственного экстремизма, и наоборот.[45] Таким образом, представляется, что иногда разные направления насильственного экстремизма находятся в симбиозе, взаимно укрепляя друг друга. Распространение правых идей насильственного экстремизма и возникающая в результате дискриминация фактически могут стать фактором, ведущим к радикализации, вдохновленной «Аль-Каидой», и

[42] http://www.transnationalterrorism.eu/tekst/publications/Rightwing%20terrorism.pdf
[43] http://www.strategicdialogue.org/RadicalRight_Conference.pdf
[44] Там же.
[45] http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1446/144610.htm

наоборот. Государства-участники ОБСЕ также признали «роль, которую преступления на почве нетерпимости, дискриминация и нетерпимость могут играть в разжигании насильственного экстремизма и радикализации, ведущей к терроризму»[46]. Однако взаимообогащение профилактических усилий, в том числе в Интернете, направленное против идеологических основ терроризма или идей правого насильственного экстремизма, пока остается ограниченным.

Сложная картина согласования и координации между правыми насильственными экстремистами и террористами

Третья сложность, которая в некоторой степени связана с двумя другими, указанными выше, заключается в неопределенности в отношении того, насколько прочно связаны и скоординированы правые насильственные экстремисты и террористы, как на национальном, так и на международном уровне, и какую роль играет в этом Интернет. Например, в отчете ЕВРОПОЛА TE-SAT 2011 года подчеркивается отсутствие единства и в целом более низкий уровень сотрудничества между правыми террористами и/или насильственными экстремистами по сравнению с другими террористическими группами.[47] При этом в недавнем отчете антирасистской группы Hope Not Hate представлена другая картина сетевой деятельности. В отчете говорится о росте масштабов деятельности и влияния на Интернет так называемых «групп борьбы с джихадом», вдохновивших Андерса Бехринга Брейвика. Важно, что ультраправые организации становятся более сплоченными по мере того, как они создают альянсы в странах Европы и в США, при этом 190 групп в настоящее время определяются как группы, пропагандирующие исламофобию.[48] Учитывая потенциальное взаимодействие между разными формами насильственного экстремизма, текущую экономическую ситуацию и пример, который мог дать таким группам Брейвик, вполне можно было бы ожидать дальнейшего сплочения и толчка, которые могут привести к актам насильственного экстремизма или попыткам вовлечь третьи стороны в политику ответных мер или внесения поправок.

Краткое описание дискуссии

Направление 1: Как правые экстремисты и террористы используют Интернет и какие тенденции можно отметить?

Хотя такие организации как ЕВРОПОЛ отмечают, что Интернет добавляет новое измерение угрозе, исходящей от правого насильственного экстремизма и терроризма, в настоящее время еще нет достаточного понимания того, как именно это проявляется.

- Эксперты отмечают рост онлайн-активности правых насильственных экстремистов. Например, один эксперт указал, что в его стране можно наблюдать тенденцию, когда правые группы все больше политизируют свои предполагаемые жалобы, обращаясь к властям, а не к объектам преступлений на почве нетерпимости, т.е. иностранцам – тенденция, которая также усиливается радикальными

[46] http://www.osce.org/cio/40695
[47] https://www.europol.europa.eu/sites/default/files/publications/te-sat2011.pdf
[48] http://www.guardian.co.uk/world/2012/apr/14/breivik-trial-norway-mass-murderer

политическими группами. Однако ответные меры на такую онлайн-пропаганду и деятельность не менее сложны, чем в отношении любой другой формы насильственного экстремизма или ксенофобии, не в последнюю очередь потому, что контент часто поступает из других стран. Продолжительное отсутствие гармонизированной международной правовой системы по-прежнему препятствует эффективному международному сотрудничеству.

- Эксперты подчеркнули, что использование Интернета правыми экстремистами не слишком отличается от других экстремистских групп. В настоящее время наблюдается три уровня онлайн-деятельности: первый уровень предполагает использование таких платформ социальных сетей как Twitter, Facebook или YouTube для размещения видеоматериалов и публикаций; второй уровень является полуоткрытым, состоящим из специальных веб-сайтов для распространения пропаганды, и определенных веб-форумов, включающих и открытые, и закрытые разделы; а третий уровень часто называют «глубокой» или «темной» сетью, состоящей из защищенных паролями форумов, которые часто спрятаны под видом архивов или сайтов-хранилищ.

- Эксперты отметили, что в последние годы происходило расширение первого уровня за счет использования методов социальных сетей ультраправыми. В качестве примера можно назвать группу Immortal в Германии, которая организуется исключительно через Twitter и другие социальные сети для проведения незарегистрированных митингов и использует YouTube для распространения записей этих собраний. Полуоткрытые форумы, такие как Stormfront, основанный бывшим лидером ку-клукс-клана в 1990-х годах, составляют второй уровень. Третий уровень состоит из форумов, защищенных паролем, таких как Legion88.

- Эксперты выяснили, что террористы, вдохновляемые «Аль-Каидой», в основном используют Интернет следующим образом:

    - Виртуальные медийные организации являются основными источниками распространения публикаций и аудиовизуальных материалов.
    - Эти веб-сайты пытаются сократить дефицит доверия между давно существующими новостными СМИ и ими самими, копируя традиционные и давно существующие медийные сайты.
    - Использование новых социальных сетей экстремистскими и террористическими сетями становится более распространенным и значительным явлением для этих групп. Существуют некоторые свидетельства, показывающие, что экстремисты типа «Аль-Каиды», применяющие насилие, используют социальные сети в рамках своей официальной стратегии.
    - Онлайн-деятельность необходимо понимать в контексте других событий, происходящих вне сети. Хотя Интернет является основным компонентом процесса радикализации, это слабый инструмент для фактической вербовки террористов в организацию и для обучения. Это почти всегда происходит за пределами сети и при личном общении.

- Интернет способствовал распространению учебных материалов, с подробным описанием всех деталей, начиная от создания самодельных взрывных устройств и заканчивая производством ядовитого газа.
- Известны случаи, когда террористы занимались онлайн-мошенничеством с кредитными картами, хищением персональных данных и другими видами незаконной деятельности для финансирования своих операций.
- Интернет дает больше возможностей для повышения активности среди женщин в таких кругах, в отличие от того, что происходит в реальной жизни.

- Эксперты установили, что использование правыми экстремистами Интернета в некоторых аспектах совпадает с тем, что делают экстремисты типа «Аль-Каиды».

    - Ультраправые веб-сайты сделаны искусно, и часто их хостинг осуществляется за пределами их целевой юрисдикции с целью избежания правовых санкций.
    - Ультраправые также используют сеть для распространения учебных пособий.
    - Есть основания полагать, что женщины более склонны к взаимодействию с правыми экстремистскими сайтами и чаще становятся активными в правых кругах, чем это могло бы происходить вне сети, хотя для подтверждения этого явления существует меньше данных.

- Эксперты также выявили некоторые четкие характеристики использования Интернета правыми экстремистами:

    - Вместо того чтобы копировать давно существующие новостные каналы СМИ для повышения доверия, ультраправые веб-сайты активно нацеливаются на молодежь, отражая образ жизни молодых людей и используя узнаваемый стиль, слоганы и символы.
    - Ультраправые используют механизмы создания отношений в сети, и появление таких новых социальных сетей и других подобных инструментов стало гораздо важнее, чем статичные веб-сайты. Главное – создать ощущение товарищества или семьи.
    - Процесс ультраправой радикализации в сети преимущественно сконцентрирован на продвижении расового нарциссизма, поддержке равнодушия по отношению к потенциальным жертвам и развитии чувства доверия и силы среди маргинальных групп.
    - Онлайн-пространство является основным источником финансирования для правых движений. Многие веб-сайты продают атрибуты, символизирующие «белую силу» и нацизм, активно развиваются интернет-магазины правого толка.

Направление 2: Какие уроки можно извлечь из онлайн-борьбы с терроризмом, вдохновленным «Аль-Каидой», в ответ на действия правых экстремистов и террористов в Интернете?

Несмотря на важность признания преступлений на почве нетерпимости и других форм крайне правого насилия в качестве отдельных вопросов, и заниматься ими на основе их четкого выделения, особенно с точки зрения обучения, повышения осведомленности, охраны правопорядка и ответных мер судебных органов, возникает вопрос о возможном дублировании функций при предотвращении таких выражений насилия и при предотвращении терроризма.

- Некоторые эксперты отметили, что концепция терроризма «одиноких волков» наиболее применима к правым насильственным экстремистам и террористам, что стало заметно в последнее время в Норвегии, и это затруднило принятие ответных мер. Ответные меры также затрудняются тем фактом, что правым экстремистам обычно менее свойственно открытое выражение насилия. Например, если форумы, вдохновляемые «Аль-Каидой», часто однозначно призывают к насилию и в результате могут быть закрыты, то правые форумы процветают, поскольку взгляды, выраженные в них, могут вызывать возражения, но часто не являются незаконными, даже если они потенциально способствуют идеям насилия.

- Эксперты отметили, что может быть полезно сосредоточиться на экстремизме, не связывая концепцию с идеологическими либо религиозными взглядами и мотивацией. Это могло бы воспрепятствовать явному сосредоточению усилий властей на той или иной группе, как это происходило в последние годы, когда некоторые формы насильственного экстремизма игнорировались или исследовались менее активно.

- Эксперты предложили ОБСЕ помочь в выявлении и усовершенствовании распространения данных о потенциальных переломных моментах, в которые экстремистские взгляды принимают насильственную форму. Идея заключается в предоставлении определенных базовых знаний, которые могут использоваться для противодействия превращению различных форм экстремизма в насильственные, независимо от причин появления экстремальных взглядов. В этом отношении также важно активизировать усилия по сопоставлению методов и выявлению общих черт между разными формами контрмер для борьбы с разными формами экстремизма, например, борьба с идеями или борьба с ксенофобскими заявлениями и выяснение, почему они являются эффективными или нет. Это позволит в будущем основать усилия на прочной базе, независимо от политического или идеологического направления новых потенциально экстремистских групп, применяющих насилие.

Форум IV: Институционализация государственно-частных партнерств (ГЧП) для борьбы с использованием Интернета в террористических целях: достижение правильного баланса между государственным и частным вкладом!

И государственный, и частный сектор считают, что эффективные ГЧП необходимы для борьбы с использованием террористами Интернета. Большая часть инфраструктуры Интернета, включая коммуникационные системы и платформы, принадлежит частным организациям, однако в руках государственных властей по-прежнему остаются основные полномочия по принятию мер в случае злоупотреблений сетью.

В реальности, однако, это взаимодействие часто бывают неравным, временным и редко получает официальное оформление. Существует ряд сложностей, связанных с таким сотрудничеством, в том числе безграничный характер Интернета; разные национальные законы, относящиеся к использованию террористами Интернета; ограниченная информированность каждой из сторон о компетентности друг друга и многое другое.

В центре находится отдельный интернет-пользователь, который одновременно играет роль «службы экстренного реагирования», выявляя использование террористами Интернета, в первую очередь в социальных сетях, и сообщая об этом, а также роль «последней линии обороны», благодаря ответственному использованию Интернета с сознательным отношением к конфиденциальной информации, что предотвращает возможные злоупотребления. Как таковые эффективные ГЧП, направленные на противодействие использованию террористами Интернета, представляют собой трехсторонние отношения между властями, интернет-компаниями и интернет-пользователями, и, как следствие, организациями гражданского общества.

Форум рассмотрел вопрос о том, как выглядят сбалансированные государственно-частные партнерства и каковы предварительные условия их существования; а также роль интернет-пользователей и гражданского общества.

Сложные задачи

Четко сформулированные принципы и законодательство

Противодействие использованию террористами Интернета может быть сложной задачей с правовой точки зрения.[49] Сама природа Интернета обусловливает необходимость

[49] Например, см. http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf

международного сотрудничества между властями, а также между правоохранительными органами одной страны и частными компаниями другой. Иногда это может приводить к конкуренции национальных законов, поскольку есть вероятность, что все они применимы к киберпространству.[50] Что касается потенциальных преступлений террористов в Интернете и связанного с ними контента, то часто возникают трудности с определением того, что является «незаконным». Определение незаконности контента может отличаться в разных странах, что в свою очередь ограничивает эффективность международного сотрудничества, например, между правоохранительными органами и интернет-компаниями. Кроме того, в некоторых случаях маркировка контента может быть слишком недальновидным решением. Например, контент, сочтенный «незаконным», может фактически не поддерживать терроризм, при этом контент, признанный «законным», потенциально может быть опасным, например, при распространении взглядов ненасильственного экстремизма[51]. Помимо юридических вопросов, государственные стратегии, относящиеся к противодействию использования террористами Интернета, также могут быть разными по объему, полноте и применимости, как и по тому, насколько о ней извещен частный сектор не только на национальном, но и на международном уровне,[52] что потенциально затрудняет оценку запросов на сотрудничество интернет-компаниями. Наконец, несмотря на наличие некоторых эффективных механизмов сотрудничества между правоохранительными органами и частным сектором на национальном уровне, в деталях они отличаются друг от друга, что затрудняет использование синергетического эффекта на международном уровне.

Четко сформулированные роли и обязанности

Проще говоря, сотрудничество между государственным и частным сектором необходимо, в частности, из-за очень четкого разделения ролей, исполняемых каждым сектором. Национальные органы власти уделяют основное внимание правовым вопросам – криминализации использования террористами Интернета или преследованию преступной деятельности при соблюдении прав человека и основных свобод. С другой стороны, интернет-компании оказывают услуги, часто концентрируясь на технических вопросах. Несмотря на то, что многие компании готовы оказать помощь в предотвращении использования террористами Интернета и в борьбе с ним,[53] в их задачи не всегда входит определение того, что является или не является законным использованием их услуг, например, в плане онлайн-контента; они не могут выступать в качестве судей, когда речь идет о вопросах частной информации, так как у них может и не быть возможностей и ресурсов для этого. Тем не менее, оба сектора заинтересованы в защите Интернета от использования террористами – и оба сектора должны честно выполнять свою часть работы для взаимной выгоды. Например, интернет-компании могут проявлять инициативу (и делают это), объясняя пользователям, что использование Интернета террористами не будет допускаться, и стимулируя сообщения о злоупотреблениях, которые они в свою очередь направляют правоохранительным

[50] Например, см. http://95.211.138.23/documents/

[51] Мнения или взгляды, которые не считаются радикальными или экстремистскими, а также их мирное выражение, не должны быть предметом правоприменительных контртеррористических мер, если они не связаны с насилием или иным незаконным действием, правовое определение которых дается в соответствии с международным законодательством о правах человека.

[52] Например, см. Отчеты по странам Совета Европы о противодействии использования террористами Интернета: http://www.coe.int/t/dlapil/codexter/cyberterrorism_db.asp

[53] Например, см. http://www.un.org/apps/news/story.asp?NewsID=33874&Cr=terror&Cr1=?ref=enews250210

органам. В то же время власти должны четко сформулировать, чего они ждут от частного сектора, с учетом ролей и обязанностей каждой стороны. Одним из наиболее очевидных вариантов, отражающих сотрудничество без вступления в область обязанностей, является повышение визуальной доступности правоохранительных органов, например, на платформах социальных сетей, в форме виртуальных полицейских проверок, чтобы напомнить пользователям о недопустимости криминального использования Интернета.[54] Аналогичным образом, назначение координаторов по использованию террористами Интернета в органах власти и в частном секторе может повысить качество постоянного обмена информацией.

Поддержание контактов с интернет-пользователями

Интернет просто слишком велик, чтобы рассчитывать, что правоохранительные органы и интернет-компании смогут эффективно реагировать на использование террористами Интернета и предотвращать его. Для этого требуется активное участие интернет-пользователей и гражданского общества. Таким образом, эффективные государственно-частные партнерства должны рассмотреть вопрос о том, как наиболее эффективно поддерживать контакты с интернет-пользователями и гражданским обществом для укрепления их роли в качестве «службы экстренного реагирования» и «последней линии обороны». В качестве «последней линии обороны», отдельные пользователи должны быть обучены ответственному сетевому поведению, разбираться в вопросах конфиденциальности и рисках, связанных с раскрытием личных данных и иной потенциально секретной информации. В качестве «службы экстренного реагирования», отдельные пользователи должны быть в состоянии определять случаи использования террористами Интернета, и получать стимулы для сообщения о подозрительной деятельности и контенте в компетентные органы и/или интернет-сервисы, в то же время сохраняя невосприимчивость в отношении террористического контента. Именно в последнем аспекте решающую роль могут сыграть организации гражданского общества. И органы власти, и интернет-компании по отдельности и совместно создали ряд механизмов и инструментов для обращения за помощью к интернет-пользователям, например, чтобы они сообщали о случаях злоупотребления или маркировали такие случаи, начиная от Справочных бюро по Интернету[55] и заканчивая возможностями маркировки на платформах социальных сетей или веб-сайтах.[56] Их эффективность, однако, не всегда очевидна. Интернет-пользователи еще не привыкли сообщать о том, что им кажется использованием Интернета террористами.[57] Более того, в случае установки возможности маркировать такой контент интернет-компании часто сами должны определять законность деятельности террористов, о которой им сообщили, например, на их платформах, и решать, о каком контенте следует сообщить в правоохранительные органы, даже если они не обладают специализированными знаниями.[58] Эффективные ГЧП, таким образом, должны не только рассмотреть вопрос о том, как разделить ответственность по установлению контактов с публикой с учетом эффективности и стратегического подхода к этому вопросу, но и то, как наиболее

[54] Например, см. http://www.dailymail.co.uk/news/article-1360908/Virtual-police-patrol-Facebook-hunt-cyber-bullies.html
[55] Например, см. http://www.reuters.com/article/2010/10/04/us-security-internet-factbox-idUSTRE6932AY20101004
[56] Например, см. http://www.facebook.com/help/search/?q=report+links
[57] Например, см. http://95.211.138.23/documents/
[58] Там же.

эффективно взаимодействовать с интернет-пользователями, чтобы реагировать на использование террористами Интернета, включая сотрудничество с организациями гражданского общества.

Краткое описание дискуссии

Направление 1: Взаимовыгодные государственно-частные партнерства

Как выглядят сбалансированные государственно-частные партнерства и каковы предварительные условия их существования? Как такое сотрудничество можно институанализировать, например, на основании общих принципов сотрудничества, в том числе на международном уровне?

- Эксперты отметили, что государственно-частные партнерства не являются «серебряной пулей», которая покончит с использованием Интернета террористами, но широко распространено мнение, что государственный и частный сектор должны работать вместе над достижением определенных целей, включая усилия по противодействию терроризму, не в последнюю очередь потому, что существующие подходы регулирования часто бывают недостаточно эффективными. Такие структуры совместного управления могут быть созданы на местном, национальном или международном уровне, концентрируясь на различных экстремистских группах и регионах. Ключом к таким усилиям является признание ролей и обязанностей каждой стороны и взаимной выгоды такого сотрудничества.

- Было подчеркнуто, что государственно-частные партнерства, основанные на проектной деятельности, обычно бывают более успешными. У них, как правило, установлены четкие сроки, что создает понимание безотлагательности среди участников, направляя их усилия в общее русло. Это также облегчает привлечение ресурсов, необходимых для достижения цели, и обеспечение поддержки высшего руководства. Благодаря установленным срокам легче избежать потенциально сложных правовых вопросов, включая положения об истечении срока действия и временные положения. К тому же успешные проекты «легче продать» руководству как в частном, так и в государственном секторе, поскольку они вносят вклад в личное профессиональное развитие людей и в достижение их целей, в связи с чем они также становятся более привлекательными.

- С другой стороны, государственно-частные партнерства, основанные на процессах, более сложны и требуют институционализации структур совместного управления. Здесь сложность заключается в создании общего восприятия проблемы, что ведет к совместному интересу к ней. Поддержка высшего руководства является важнейшим моментом для того, чтобы заложить основу и придать силы партнерству в моменты сбоев в управлении. Моменты активизации дают возможность инициировать и оформить такие партнерства. Важно, чтобы ценность существовала для обеих сторон, и участники видели эффективность своих затрат времени и ресурсов.

- Ключевым элементом успешного сотрудничества является установление доверия между должностными лицами частного и государственного сектора. Для этого требуется открытость со стороны участников, чтобы они могли работать вместе, а это является обязательным условием для преодоления первоначального недоверия. Кроме того, существуют четкие ограничения эффективного развития доверия внутри социальной группы: чем больше членов в группе, тем тяжелее установить и в течение длительного времени сохранять доверие. Успешная институционализация партнерства, таким образом, требует от группы людей в течение времени регулярно взаимодействовать и работать совместно и, что особенно важно, доверять друг к другу.

- Было отмечено, что не регулируемые законом «системы», такие как Clean IT Project, могут способствовать развитию устойчивого и эффективного сотрудничества. По сути, интернет-отрасль, НГО, правоохранительные органы и государственные организации согласны в отношении основных принципов и передовой практики, относящихся к противодействию использованию террористами Интернета, что является основой для будущих усилий и заполняет пробел между (государственным) регулированием и частными инициативами и передовой практикой. Ключом к разработке таких принципов и рекомендаций является включение общественности в обсуждение и обеспечение наибольшей прозрачности процесса, чтобы все стороны могли согласиться с определенным набором принципов и внедрить их. Эксперты все же подчеркнули, что в некоторых случаях и в определенных ситуациях требуются более формальные соглашения.

Направление 2: Роль интернет-пользователей и гражданского общества

Как более эффективно задействовать интернет-пользователей и гражданское общество? Каковы существующие примеры передовой практики и как улучшить существующие инструменты и механизмы привлечения отдельных интернет-пользователей?

- Помимо потенциального вклада, отмеченного на предыдущих форумах, эксперты вновь подчеркнули потенциальную важность интернет-пользователей и гражданского общества в борьбе с онлайн-экстремизмом. Хорошим примером является сеть Against Violent Extremism («Против насильственного экстремизма»). Она является дочерним проектом более крупной государственно-частной инициативы, развиваемой Google Ideas, рабочей группы по выработке идей и действий, созданной Google с целью служения обществу. Более конкретно, речь идет о глобальной сети бывших насильственных экстремистов, свидетелей, активистов, политиков и бизнесменов, объединенных общей целью: борьбой с насильственным экстремизмом. Бизнес-модель состоит в том, что каждый год эта организация занимается одной определенной темой, созывает крупную встречу на уровне экспертов, а затем направляет свою энергию в институализированную организационную структуру, которая продолжает заниматься этой темой на более

долгосрочной основе. Таким образом, они начинают с работы на основе проектной деятельности, а затем переходят к сотрудничеству в рамках процесса. Здесь также сочетаются глубокие знания социологии и доверие, возникающее между небольшими группами людей, и структурированный сетевой подход к обеспечению широкой сферы действий.

- Было подчеркнуто, что другой способ, с помощью которого пользователи могут внести свой вклад в противодействие использованию террористами Интернета, имеет форму волонтерства или общественно-полезной деятельности в рамках краудсорсинга. Сюда может включаться активное стимулирование других людей к тому, чтобы они сообщали о злонамеренной деятельности.

- Эксперты подчеркнули, что одним из основных препятствий для сообщения об использовании террористами Интернета было то, что механизмы передачи таких сообщений преимущественно ограничивались государственными границами. Эксперты предложили, чтобы такие международные организации как ОБСЕ рассмотрели вопрос о том, каким образом можно перевести такие механизмы в международную или централизованную плоскость, чтобы контент, о котором сообщают пользователи, автоматически передавался компетентным государственным органам. Кроме того, важно стандартизировать и упростить механизмы передачи сообщений, чтобы пользователи действительно могли применять их.

Organization for Security and Co-operation in Europe