СЕТЕВЫЕ ТЕРРОРИСТИЧЕСКИЕ СООБЩЕСТВА

Климашин Александр Геннадьевич
Институт социологии НАН Беларуси, Минск

Сегодня в мире наблюдаются серьёзный скачок технологического развития. Наука развивается «по экспоненте», то есть чем больше открытий, тем больше производится новых достижений и исследований. Сегодня реальную революцию в производстве представляет 3D-печать, дроны (беспилотники и роботизированные механизмы), когнитивные технологии. В недалекой перспективе эти технологии повлияют серьёзным образом на жизнь общества, так как в корне изменят способ производства, что вероятнее всего вызовет социальную напряженность из-за сокращения рабочих мест и ликвидации мелкого предпринимательства. Вторая опасность в том, что рассматриваемые технологии имеют двойное назначение, а точнее не подлежат точной классификации в соответствии с принципом прямого назначения.

Несмотря на широкий спектр технологического развития, практически все эксперты единогласно характеризуют XXI век, как век цифровых технологий и связывают его с информатизацией экономики. Такое единодушие вызвано тем, что интернет как явление проник во все сферы жизнедеятельности человека, а также стал ключевым базисом для дальнейшего производства высокотехнологичных продуктов. Большая часть «умных вещей», беспилотных и роботизированных устройств управляются по средствам глобальной сети.

Наиболее явные черты нашей эпохи – это избыток информации и открытость основной части общества. Вместе с тем, открытость общества и новые возможности коммуникации не сделали мир добрее, как того бы хотелось. Не требует подробного описания и доказательства проблема террористической угрозы. В ходе проведения Национального форума по управлению интернетом (IGF-2017) на базе Mariott Hotel, организованного при поддержке ICANN, ООО «Хостер бай», Human constanta и другими известными компаниями, участниками по результатам опроса наиболее остро были востребованы вопросы «Защиты персональных данных», «Безопасность в интернете».

С одной стороны, при появлении и развитии международной сети Интернет встала проблема соблюдения прав человека и национальной безопасности, потому что известные субъекты осуществляют слежение за неопределённым кругом лиц вопреки процессуальному законодательству. С другой стороны, даже такие мероприятия не позволяют предотвращать террористические акты и наращивание потенциала террористических движений. Фактически обе проблемы трудно разрешамы в силу того, что их решения противоречат друг другу. По сути это новая плоскость спора правозащитных организаций и так называемого «силового блока».

Почему вообще возможна коммуникация между террористами и вербовка новых членов в группы? Один из известных способов конспиративной связи по средствам сети Интернет являются компьютерные онлайн-игры. Большая часть сообщений идёт через игровую консоль, в которой технически невозможно

фильтровать трафик. Следующий аспект связан с многочисленными социальными сетями. Открытость данных позволяет не только специальным службам, но и злоумышленникам получать данные о потенциальных жертвах преступлений и потенциальных агентах преступного сообщества. Сегодня для поиска информации о человеке не требуется специальной техники и большого объема специализированных знаний. Для установления личности требуется только усидчивость и высокоскоростное соединение. Изучение политических взглядов и убеждений весьма просто по комментариям, статьям в блогах, опубликованным научным статьям. Более того с потенциальной жертвой очень просто вступить в коммуникацию. Фильтровать трафик таких сообщений так же весьма сложно. Во-первых, это будет усложнять проблему соблюдения прав человека, во-вторых это слишком большой объём работы, так как на подсознательном уровне и в приватных беседах проследить склонности к смене общественного строя можно у многих, но преследовать людей лишь за умысел было бы не совсем правильно. Как отмечает руководитель специальной следственной группы Следственного комитета Республики Беларусь по киберпреступности Александр Сушко, наибольшую проблему в расследовании этих дел представляет их осложнённость иностранным элементом. Ведь преступник, даже не находясь за пределами государства, в своих деяниях пользует иностранными прокси-серверами; сервера социальных сетей «ВКонтакте», «Facebook» и так далее также находятся в юрисдикции других государств. Поэтому для установления местонахождения преступника и получения свидетельств об этом требуется активная коммуникация соответствующих органов на международном уровне. Но такая коммуникация не всегда возможна в силу закрытости специальных служб, межгосударственных противоречий, отсутствия опыта совместной работы и так далее. В Республике Беларусь для разрешения подобных проблем была создана специальная группа – Национальный центр по реагированию на компьютерные инциденты при Оперативно-аналитическом центре (CERT). Среди задач группы не только бороться с киберпреступностью, но и отладить механизм по работе в этой сфере. Как отмечает руководитель группы, сложность работы во многом в том, что компьютерные инциденты как правило выражаются в новых и новых формах. Поэтому при появлении нетипичных событий действовать требуется скорее в соответствии с профессиональной интуицией, нежели по предписанным правилам.

Правозащитный подход к проблеме заключается в том, что специальные службы должны больше концентрироваться на работе в реальной жизни, чем в цифровом пространстве, так как в противном случае это неизменно ведёт к тому, что в процессе оперативно-розыскных мероприятий происходит нарушение прав человека и незаконным образом отслеживается его личная переписка. В США после инцидента с участием Эдварда Сноудена была создана специальная комиссия из судей, которая задала соответствующие вопросы Директору АНБ. Последний признался в том, что в процессе специальной деятельности проводится сбор личных данных, как иностранцев, так и граждан

США. Однако он сказал, что это происходит неумышленно, а в силу специфики технологического процесса. То есть, например, при выявлении покупателей оружия могут мониториться поисковые запросы в системе Google, но вместе с таким мониторингом корпорация собирает и хранит поисковые запросы всех остальных граждан. Подобные технологические возможности в США привели к тому, что уже неоднократно возникали судебные споры с участием Google, Apple по подозрению их в установлении средств негласного получения информации на свою продукцию для дальнейшего обмена этих данных с АНБ и ЦРУ. При этом даже такие беспрецедентные меры не привели к снижению уровня террористической угрозы и снижению количества актов терроризма ни в США, ни в мире, а скорее, напротив. Почему так происходит?

На самом деле ответ очень прост. При внедрении технологий разработчик всегда исходит из того, что этими технологиями будут пользоваться для гражданского назначения, а их использование будет добросовестно регулироваться источником власти как «ночным сторожем». Но на практике это так не работает и никогда не работало. Это глубокое заблуждение. Вопрос наличия преступных группировок, организованных преступных сообществ всегда зависел всего от двух факторов: 1) наличие чёткого мотивированного убеждения по смене текущего общественного строя; 2) доступ к ресурсу (оружию, персональным данным, потенциальным участникам группировки, деньгам). Очевидно, что оба фактора в большей степени проявились с развитием технологий Интернета. Мотивация во многом вызвана развитием цифровых технологий. Сегодня крайне тяжело реализоваться в реальной жизни, зато очень просто в виртуальном мире. Автоматизация труда привела к огромному сокращению числа рабочих мест. Поиск супруга осложнился увеличением конкуренции за счет миллиардов виртуальных собеседников. Избыток ненужной и противоречивой информации вызвал у молодёжи сильный мировоззренческий кризис. Широкий доступ к порнографии, чуждым ценностям, альтернативным мнениям об истории зародил в личности закономерные сомнения о ценностях прошлых поколений. Озлобленность на такую реальность ставит людей в оппозицию к общественному строю, а посредствам интенсификации общения в социальных сетях и онлайн играх создаёт благоприятную почву для вербовки личности в деструктивные течения. Доступ к ресурсу также стал более простым, чем в прошлые столетия. Не достаточно перекрыть точки торговли оружием в реальной жизни и отслеживать их. В принципе, любой желающий может посмотреть и соорудить самостоятельно необходимые приспособления, не говоря уже о полноценной 3D-печати оружия. Узнать о потенциальных сбытчиках так же стало куда проще по средствам сети Интернет. Очевидно, что торговля «спайсами» статистически, даже в Беларуси с её достаточно жестким законодательным регулированием, за 2015–2016 годы значительно выросла за счёт сбыта через социальные сети. Перекрытие публичных домов тоже стало более затруднительным за счет сложности их обнаружения без отслеживания через сеть Интернет. Кроме того, глобальная система Интернет позволяет

практически любому субъекту за низкую плату использовать средства негласного получения информации, что так же, как и многое вышеприведенное способствует развитию преступных сообществ. Но если прочее выступает средством одурманивания и подрыва ценностей, то gps-маячки и камеры могут служить средством обеспечения совершения таких преступных посягательств, как кража денежных средств и слежка за местом проведения террористического акта. Подобные маяки могут выступать и детонаторами взрывных устройств, имея при этом управление не через мобильные сети, а через точки доступа к виртуальной сети.

Что же касается террористических группировок, то схема вербовки выглядит примерно следующим образом:

1) вербовщик выявляет лиц из числа граждан страны «противника» – оппозиционеров и лиц с неудачной карьерой по сообщениям в прессе, высказываниям в комментариях, блогах и социальных сетях;

2) далее кандидатура на вербовку подвергается тщательному анализу и изучению. Устанавливаются его возраст, пол, адреса, телефоны, почта, родственники, круг друзей и коллег. Изучается психологический портрет и способы воздействия на объект;

3) после этого следует процедура вхождения с объектом в контакт по средствам социальных сетей, и осуществляется негласное собеседование с кандидатом;

4) при наличии склонности к зарабатыванию денег на совершении преступных посягательств кандидату предлагается или совместное путешествие или компьютерная игра, где и вносятся предложения по сотрудничеству;

5) конечно, как правило, кандидат перепроверяется «на вшивость» путем участия в проверочных правонарушениях на территории третьих стран с последующим обучением и хорошей заработной платой за веру в «священную войну» против политического устройство сего мира.

Стоит отметить, что подобная схема является достаточно универсальной для большинства радикальных течений. Во-многом потому, что общение через Интернет и социальные сети рядовым гражданам наиболее понятный способ социальной коммуникации.

В идеологическом и мировоззренческом плане решение видится в том, что в первую очередь появление новых цифровых технологий не должно заменять реальной жизни. Это, скорее, должно быть дополнительной возможностью и дублированием неких функций. Но стоит опасаться полной замены административных функций «электронным правительством», полной замены оплаты электронными платежами, полной замены реального общения – социальными сетями. Способы социальной коммуникации должны развиваться и давать человеку выбор, но ни в коем случае не вгонять его в рамки нового мирового порядка. Именно тогда человек как личность, сможет быть более самодостаточным и независимым от какой-либо системы.

Что же касается технологических мер по защите от киберпреступности и вербовки в преступные сообщества посредством сети Интернет, то вопрос остается, и, скорее всего, будет оставаться открытым долгое время. Ведь любая мера по идентификации абонента в сети сопряжена с получением его персональных данных системными администраторами и правоохранительными органами. Эти данные зачастую касаются самых интимных сторон жизни человека. Но при отсутствии таких правовых и технических механизмов всегда возникает угроза девиантного поведения субъекта. Именно поэтому несколько лет назад на уровне ООН заговорили о разработки Модельной Конвенции по управлению интернетом. Однако до сих пор взвешенного правового решения не найдено. Главной проблемой остается описание механизма взаимодействия различных субъектов в процессе управления интернетом. На наш взгляд, в силу того, что Интернет дублирует всю текущую реальность в цифровом поле, невозможно отрегулировать жизнедеятельность человека одной лишь конвенцией. Решением видится скорее адаптация всего законодательства под те реалии, которые нам предлагает сетевая жизнь. Кроме того, и сами субъекты должны с большей осторожностью относиться к защите своих данных, ибо в случае игнорирования, например, правил перехода через проезжую часть, ГАИ не может гарантировать вашу безопасность. Так же и тут. Не стоит, да и невозможно отказаться от благ современной науки, но при этом не стоит попустительствовать банальными мерами предосторожности. Любой пользователь Сети должен с уразумением относиться к сомнительным социальным сетям, где просят ввести телефонный номер, номера банковских карточек и (или) пароли от почты. Также с осторожностью стоит относиться к сомнительным предложениям в социальных сетях, если вы работаете с официального своего аккаунта, который помогает вас идентифицировать.

Вообще стоит отметить, что сегодня куда более популярными стали так называемые мессенджеры: Viber, Skype, Telegram, WhatsUp, WeChat. Во-первых, они более просты в использовании и требуют меньшего количества времени. Во-вторых, они в большей степени гарантируют безопасность за счет трёх факторов: 1) привязки к номеру мобильного телефона (все, кроме Skype); 2) сильного алгоритма шифрования; 3) нехранения переписок на серверах (по словам разработчиков Telegram, Viber). Привязка к номеру мобильного телефона обеспечивает сразу несколько условий защищённости. Вам не напишет никто, у кого нет вашего номера и в то же время, если вам пишет какой-то номер, то вы уверены, что это именно этот номер, а не фейковый аккаунт, созданный специально для неких преступных целей. Кроме того, мессенджеры содержат только необходимую базовую персональную информацию об абоненте. Ранее наиболее безопасным продуктом представлялся Viber, так как имел белорусских разработчиков, и до недавнего времени сервера находились в пределах национального сегмента сети Интернет.

Таким образом, можно сделать вывод, что технологии сильно меняют наше общество. Они делают многие процессы более удобными. Но вместе с тем, мир не становится добрее, и наряду с появлением новых технологий возникает

необходимость разработки новых защитных мер. Этот вопрос касается и технологической стороны и мировоззренческой, так как вместе с новым образом жизни, меняется и образ мыслей человека, возникают новые бытовые проблемы и новые социальные конфликты.

Список литературы

1) *Воронович, В*. Основные причины, предпосылки и факторы распространения терроризма в XXI в. / В. Воронович // Журн. междунар. права и междунар. отношений. – 2005. – № 4. – С. 39–45.

2) *Брюхнов, А. А*. Некоторые вопросы классификации проявлений терроризма в современном обществе / А. А. Брюхнов, Н. А. Вакуленко // Философия права. – 2016. – № 1. – С. 73–77.

3) *Дикаев, С. У.* Террор, терроризм и преступления террористического характера: криминологическое и уголовно-правовое исследование / С. У. Дикаев. – СПб: Юрид. центр Пресс, 2006. – 448 с.

4) *Капитонова, Е. А.* Современный терроризм / Е. А. Капитонова, Г. Б. Романовский. – М.: Юрлитинформ, 2015. – 214 с.

5) *Климашин, А. Г.* Современные подходы к пониманию общественно-экономической формации. Ноосферная экономика // Беларусь на пути прогресса: инновационная экономика, управление, право / А. Г. Климашин. – 2008. – С. 118–120.

6) *Кузнецов, А. П.* Международный терроризм в условиях глобализации / А. П. Кузнецов, Н. Н. Маршакова // Юридический мир. – 2010. – № 9. – С. 8–12.

7) *Курцвейл, Р*. «Эволюция разума» / Р. Курцвейл. – М.: Эксмо, – 2016. – 320 с.

8) *Трошин, В. Д*. Терроризм и нервно-психические расстройства: диагностика, лечение и профилактика / В. Д. Трошин, Т. Г. Погодина. – Нижний Новгород: НГМА, 2007. – 312 с.

9) *Павлинов, А. В.* Криминальный антигосударственный экстремизм: уголовно-правовые и криминологические аспекты: автореф. дис. ... д-ра юрид. наук: 12.00.08 / А. В. Павлинов ; Ин-т государства и права Рос. акад. наук. – М., 2008. – 56 с.

10) *Хантингтон, С*. Третья волна: демократизация в конце XX века / С. Хантингтон. – М.: РОССПЭН, 2003. – 368 с.

11) *Хоффман, Ф*. Гибридная война и ее вызовы / Ф. Хоффман // Мировойна. Все против всех: новейшая концепция боевых действий англосаксов / сост., введ., заключение Е.С. Ларина, В.С. Овчинский. – М., 2015. – С. 182–190.