**ТЕРРОРИЗМ В ИНТЕРНЕТЕ**

Современное общество – это общество информационное. Сейчас каждый человек может овладеть любой информацией и в огромном количестве. Казалось бы, люди достигли совершенства знания – доступно все, все можно узнать – надо только зайти в Яндекс или погуглить. Главное, правильно ввести запрос. Но не всякое знание несет настоящее знание и не всякая информация полезна. Информационная революция вместе со всеми преимуществами принесла и серьезные проблемы в сфере общественной безопасности. В первую очередь это касается распространения терроризма в Интернете. По данным Национального антитеррористического комитета РФ, в настоящее время в мире действует около 5 тысяч интернет-сайтов, активно используемых террористами. Число порталов, обслуживающих террористов и их сторонников, постоянно растет.

В одной из статей о терроризме, опубликованной в США в 2000-е годы, была такая фраза: "Если и есть что-то, что ФБР ненавидит больше, чем Усаму бен Ладена, так это то, когда Усама бен Ладен начинает пользоваться Интернетом". Действительно, терроризм – это страшное и глобальное явление уже само по себе, а когда террористы используют еще и глобальную сеть как оружие воздействия на массы – получается вдвойне страшно. Терроризм в Интернете – очень динамичное явление, веб-сайты и страницы в соцсетях внезапно появляются, часто меняют формат, а затем так же стремительно исчезают. Во многих случаях это лишь видимость исчезновения, меняется лишь адрес сайта, содержание остается прежним. Зачастую террористические сайты имеют зарубежного провайдера, поэтому на практике получается, что их не так-то легко закрыть. Так Россия уже несколько лет "гоняется" за террористическо-экстремистским сайтом "Кавказ-центр", который упрямо "путешествует" из страны в страну близ российских границ (в зависимости от отношения той или иной страны к России), и остается только блокировать доступ к нему в самой России в рамках антитеррористического законодательства.

По своей природе Интернет во многих отношениях – идеальное поле деятельности террористических организаций. Всемирная сеть привлекает возможностью свободного доступа, невысокой стоимостью связи, слабостью (а часто отсутствием) цензуры и какого-либо государственного контроля, относительной анонимностью (что важнее всего), быстрой передачей информации, огромной аудиторией, техническими возможностями, наконец.

Каково содержание террористических сайтов? Как правило, сайт содержит информацию об истории организации и ее действиях, детальный обзор социальных и политических вещей, пропаганду, отчеты об "акциях", иногда биографию лидеров, основателей и "героев", сведения о политических и идеологических целях, жесткую критику врагов, и текущие новости. Все это - "в собственном изложении".

Зачастую террористическая организация изображается как постоянно преследуемая: якобы ее лидеры подвергаются попыткам убийства, последователи арестовываются, свобода выражения ограничивается. Такая тактика, изображающая организацию маленькой, слабой и преследуемой мощью сильного государства, рассчитана на привлечение «сочувствующих» последователей. Члены движения или организации представляются "борцами за свободу", использующими насилие против их желания, потому что "безжалостный враг" "ущемляет права и достоинство людей". Соответственно, в качестве "настоящего террориста" там позиционируется враг террористического движения или организации – к примеру, очень часто можно встретить тезис типа “Наше насилие ничтожно по сравнению с его агрессией”. Это наиболее общий аргумент. Террористы перекладывает ответственность за насилие с себя на противника, который обвиняется в демонстрации зверства, жестокости и безнравственности. Действительно, есть Женевская декларация "О государственном терроризме", где к таковому отнесена практика "полицейского государства", некоторые юристы отмечают косвенное признание Всеобщей декларацией прав человека "права на восстание" - только вот одна проблема: к практике и идеологии террористических групп и движений все эти ссылки обычно не имеют никакого отношения, так как они сами грубейшим образом нарушают базовые права и свободы человека. То, что "насилие в ответ на насилие" не есть оправдание, установил еще Нюрнбергский трибунал.

Надо сказать, в пропагандных целях ресурсы террористов часто пытаются подстроиться под интересующую их аудиторию. Если пропагандистский сайт террористов рассчитан на западного потребителя, то внешне он будет выглядеть вполне "демократически" - материалы сайта продемонстрируют "ориентированность" на западный путь развития, строительство нового общества с учетом (а то и на основе) западных гуманистических ценностей с признанием нерушимости демократических прав и свобод, частной собственности и свободной рыночной экономики. Однако надолго этого "камуфляжа" редакторам сайтов, как правило, не хватает - в текущих материалах истина мгновенно выплывает наружу. А разговоры про "гуманистические ценности" остаются только в "камуфляжном" программном документе.

То, что террористы используют информационную (и не только) открытость цивилизованного мира для реализации своих целей, уже давно не секрет - об этом писал еще Артур Хейли в 1990-м году (пример, как легко террорист сделал себе паспорт). Раньше, до Интернета, им было труднее организовывать и исполнять террористические акты из-за расстояния и необходимости координировать действия. Сейчас таких проблем у них технически в разы меньше. С помощью Интернета преступники могут согласовать время, место проведения терактов. В некоторых случаях Интернет может помочь свести к минимуму "рекогносцировку на месте" - картографический сервис в этом плане дает очень широкие возможности для всех пользователей Интернета без исключения, предоставляя в открытом доступе спутниковые снимки и карты любой местности. При террористической атаке в индийском городе Мумбаи террористы активно использовали именно картографический сервис - и благодаря подробностям, которые можно изучить с его помощью, террористы планировали свои действия. Поэтому в свое время калифорнийские конгрессмены предложили некий закон, согласно которому в Google Maps нужно размывать изображение определенных областей, чтобы их нельзя было детально изучать. К таким объектам относятся школы, церкви, больницы и правительственные сооружения. Вместо них законодатели предлагают созерцать цветные размытые пятна. Нововведение не запрещает людям определять направление маршрутов, но вентиляционные отверстия и лифтовые шахты не должны отображаться на экране. Но не следует забывать, что и без предлагаемого Google сервиса, достать карты интересующей местности в наше время не составляет труда. Со спутниковыми снимками немного сложнее, но и их при желании достать вполне возможно.

Страшнее всего то, что боевики размещают на сайтах руководства по изготовлению бомб, оружия, организации терактов и тому подобного. Владельцы сайтов, которые вывешивают подобные инструкции, пытаются избежать наказания, утверждая, что не они являются авторами руководств и что они не призывают использовать данную информацию на практике. В некоторых случаях - когда не удается установить конкретное лицо, распространившее информацию - им это вполне удается. Риск же закрытия сайта или страницы в соцсети их особо не смущает...

Отдельная тема - компьютерный терроризм. Проще говоря, террористы могут атаковать или проникнуть внутрь компьютерных систем различных учреждений. Последствия этого могут быть разнообразные: пострадать могут военные, разведывательные, медицинские службы, транспортные и финансовые системы...  Потенциальные масштабы кибертерроризма ужасны, поскольку они могут внести хаос в действия не только государственных, но и коммерческих структур, парализовав, например, банковские операции. Самая, пожалуй, значимая история в этом плане - попытка заражения специальным вредоносным ПО оборудования строящейся иранской атомной электростанции (если бы все получилось, то масштабы последствий можно себе представить по фотогалереям города Припять у Чернобыльской АЭС).

Чтобы воздействовать на людей, террористы используют "психологические атаки", которая заключается в распространении угроз. Цель очевидна: посеять страх и ощущение беспомощности. Частое средство -  распространение ужасающих изображений своих действий, например, видео казни заложников. В свое время американское общество потрясла видеозапись убийства американского журналиста Дэниэла Перла лицами, захватившими его в плен, которую выложили на нескольких веб-сайтах. Террористы также могут начать психологические атаки посредством кибертерроризма, а точнее, создания опасений угрозы совершения таких действий. “Киберстрах” возникает из беспокойства об угрозе компьютерных нападений (например, падения самолетов, вывода из строя систем управления воздушным движением, сбоев в системе национальной экономики путем нарушения компьютерных систем, регулирующих фондовые биржи и т.п.), которое усиливается настолько, что общество начинает верить, что атака случится.

Как и другие политические организации, террористические группы используют Сеть для пополнения фондов. С помощью сети руководители террористических сайтов осуществляют сбор денежных средств на поддержку преступных операций, на содержание боевиков.Правда, в последние годы с этим стало значительно сложнее - на это есть и действуют соответствующие международные конвенции...

Террористы используют в своих целях и рекламные возможности сети. Им очень выгодно предавать своим действиям гласность, не привлекая при этом телевидение, радио или печатные СМИ, что сделать гораздо сложнее. Делается это для запугивания потенциальных врагов. Чтобы привлечь сторонников, а главное, молодежь, сайты террористических организаций часто выполняют функции интернет-магазинов: они предлагают купить флаги, футболки, плакаты, значки, аудио- и видеозаписи с их символикой.

Интернет стал благодатной почвой и для распространения слухов. Теракты, совершенные в Москве весной 2010 года, активно обсуждались в чатах, блогах и форумах: очевидцы или участники становились чуть ли не «звездами», пытаясь поделиться пережитыми впечатлениями, порой приукрашивая свершившееся. В сети стали появляться слухи об организации теракта, его руководителях. Некоторые из них были очень далеки от реальности, тем не менее получали поддержку общественности.

Таким образом, террористическая активность в Интернете – четко спланированное психологически направленное воздействие на население, и организовывают его специально подготовленные люди, обладающие определенными знаниями. Именно они направляют «толпу», особенно воздействуя на тех, кто имеет несформировавшееся мировоззрение, и кто не определился со своим предназначением в жизни.

Как бороться с терроризмом? Тем же методом – информированием. Террористы используют ложную информацию с целью вербовки. У мирного населения должно быть информирование с целью знания – что такое терроризм, как он проявляется в Интернете, какие сайты существуют, какова их цель, к чему приводит участие в подобных группировках и прочее. Человека знающего и осведомленного не так просто сбить с толку.

Поскольку терроризм - проблема обычно международная, с терроризмом надо бороться на мировом уровне - развивать сотрудничество в области правовой взаимопомощи, обмена разведывательными данными. Необходимо все-таки довести до логического конца международное законодательство по борьбе с преступностью в компьютерной сфере с тем, чтобы пресечение компьютерных преступлений минимально зависело от национальных границ. Задача же правоохранительных органов во всех странах остается та же: изучение и пресечение террористических действий в Интернете, а также поиск мер по ограничению использования этой среды современными террористами.

Правда, здесь есть другая опасность, которую вполне справедливо именуют "антитеррористическая паранойя". Под эгидой "борьбы с терроризмом" государство может начать массовый ввод практик и законов, которые довольно серьезно нарушают права и свободы человека и гражданина - или как минимум создают людям огромные неудобства. В некоторых случаях речь идет действительно о чрезмерной перестраховке законодателя или правоприменителя, но в других случаях интересующие ограничения и нарушения прав граждан просто "протаскиваются" под поводом "борьбы с терроризмом". Негативные последствия, в том числе в антитеррористической работе, очевидны с различных сторон. И в Интернете тоже. Таким образом, грамотное противостояние террористической угрозе - дело исключительно тонкое и требующее огромной компетентности...