**Терроризм и интернет**

Интернет стал одной из причин возникновения "нового вида терроризма" – когда, не имеющие единого штаба организаций, объединены сетями электронных коммуникаций.  Многие террористические организации создали в Интернете базы разведывательных данных, которые используются при подготовке атак. Известно, например, что японская террористическая группировка "Аум Синрике", которая провела газовую атаку в токийском метро в 1995 году, перед этим создала компьютерную систему, которая была способна перехватывать сообщения полицейских радиостанций и отслеживать маршруты движения полицейских автомобилей.

Деятельность террористов в Интернете можно классифицировать следующим образом:

* "активизм",
* "хакеризм"
* "кибертерроризм".

Активизм - это "легитимное" использование киберпространства для пропаганды своих идей, зарабатывания денег и привлечения новых членов. Хакеризм - хакерские атаки, проводимые для выведения из строя отдельных компьютерных сетей или интернет-сайтов, получения доступа к секретной информации, хищения средств и т.д. Кибертерроризм - компьютерные атаки, спланированные для нанесения максимального ущерба жизненно важным объектам информационной инфраструктуры.

Чаще всего террористы используют Интернет для связи, пропаганды, привлечения сочувствующих. Здесь террористы вполне преуспели.

Всемирная Сеть является идеальной средой для деятельности террористов, поскольку доступ к ней крайне легок:

* в Интернете просто обеспечить анонимность пользователей,
* Интернет никем не управляется и не контролируется,
* в сети Интернет не действуют законы и не существует полиции.

Если в 1998 году примерно половина из 30-ти организаций, которых США причисляли к террористическим, обладали своими сайтами, то ныне в Сети представлены абсолютно все известные террористические группы, которые публикуют свои материалы, по меньшей мере, на 40 различных языках.

Вероятно наиболее опасным способом использования Интернета является размещение на сайтах руководств по изготовлению бомб, оружия, организации терактов. Пионерами в этом деле были анархисты, которые еще в 1950-е годы создали подобное пособие "Поваренная Книга Анархиста", которую с конца 1980-х годов активно популяризуют в Интернете. Владельцы сайтов, которые вывешивают подобные инструкции, обычно избегают наказания, утверждая, что не они являются авторами руководств и что они не призывают использовать данную информацию на практике.

Терроризм в Интернете опасен тем, что террористы могут атаковать или проникнуть внутрь компьютерных систем, принадлежащих важнейшим государственным структурам. Последствия этого могут быть разнообразные: пострадать могут военные, разведывательные, медицинские службы, транспортные и финансовые системы и т.д.

Допускается возможность совершения теракта лишь с помощью компьютера. Прецеденты этому уже существуют. К примеру, в 1998 году 12-летний хакер взломал систему доступа к пульту управления дамбой одного из крупнейших водохранилищ США. Фактически, школьник получил дистанционный контроль над системами водосброса. Если бы он отдал команду полностью открыть затворы, то под лавиной воды погибли бы жители, как минимум, двух близлежащих городков.

Террористы уже использовали или в состоянии использовать такие виды "кибероружия", как компьютерные вирусы, "черви" и "троянские кони", "логические бомбы" и т.д. Однако на сегодняшний день наиболее популярным и заметным видом кибертерроризма является взлом сайтов и размещение на них лозунгов и призывов.

**Существует несколько возможных способов, с помощью которых можно использовать Интернет в целях содействия террористическим группам:**

* С помощью **Интернета** можно осуществлять сбор подробной информации о предполагаемых целях, включая изображение местонахождения целей и их характеристики. Если террорист в состоянии получить ключевую информацию по предполагаемой цели высокой степени важности, например, трубопровод или силовая подстанция, то он может контролировать или шантажировать предприятия или даже правительство.
* С помощью **Интернета** можно осуществлять сбор денег для поддержки какого-либо движения или манипулировать ценными бумагами с тем, чтобы обогатиться на них после осуществления террористического акта. Один из сайтов, посвященных целям и задачам Чеченской Республики в борьбе по отделению от России, адресует читателей к банку в г.Сакраменто (штат Калифорния) и предоставляет номер счета, на который можно послать деньги для поддержки усилий чеченцев по выдворению русских из республики.
* . **Интернет** может собрать воедино различные группы людей по характерным признакам. С помощью сайта в Интернете можно давать указания о времени и месте проведения встречи, формах протеста или вопросах для изучения. Таким образом, Интернет оказывает объединяющее воздействие на деятельность таких групп.
* **Интернет** можно использовать и для осуществления нападок на отдельные лица, группы людей. Вымогатели используют Интернет для того, чтобы требовать деньги
* **Интернет** обладает огромным рекламным потенциалом и часто используется в этих целях. С помощью Интернета можно мгновенно обратиться как к массовой аудитории по всему миру.
* . Благодаря **Интернету** терроризм уже не ограничен лишь государством, где скрываются террористы, им не надо предъявлять паспорт. Более того, базы подготовки террористических операций уже, как правило, не располагаются в странах, где находятся цели террористов.
* . **Интернет** может служить в качестве инициатора психологического терроризма. Часто психологическим аспектам возможностей Интернета не уделяют должного внимания. Благодаря кажущейся надежности и высокой репутации, которой якобы обладает Интернет, его можно использовать для того, чтобы посеять панику, ввести кого-нибудь в заблуждение или привести к разрушению чего-либо. Интернет также стал подходящим местом и благодатной почвой для распространения слухов.
* . **Интернет** существенно изменил коммуникационную сеть террористов. Если ранее это были сети с сильным центральным командным пунктом, то теперь это сети, где четких командных пунктов не просматривается благодаря еще большему развитию сетевого характера этих структур. Ничего не подозревающие соучастники, например хакеры, могут быть использованы "втемную", как подставные лица. Они могут никогда не узнать, к чему в конечном итоге привели их действия.
* . **Интернет** может быть использован и для отправки сообщений тайным образом, что похоже на то, как ранее использовались симпатические чернила.

По своей природе Интернет во многих отношениях – идеальное поле деятельности террористических организаций. Особенно это касается предлагаемых глобальной сетью:

* Свободного доступа
* Небольшие регулирование, цензура и другие формы государственного контроля или вовсе их отсутствие
* Потенциально огромная аудитория во всем мире
* Анонимность связи
* Быстрое движение информации
* Невысокая стоимость создания сайта и обслуживания присутствия в сети
* Мультимедийная среда: возможность комбинировать текст, графику, аудио и видео, возможность для пользователей загружать фильмы, песни, книги, постеры и т.д.
* Возможность охватить также аудиторию традиционных СМИ, которые все чаще используют Интернет как источник сообщений.

**Заключение**

К террору нельзя привыкнуть. Общество, в котором “эстетика” террора находит отклик или понимание у значительной части населения, обречено на тяжкие испытание.

Слова старого чеченца, приведённые в одной из газет после вторжения в Дагестан банд формирований, как нельзя лучше характеризуют суть этой сложной проблемы: “Мы в детстве играли в Чапаева, а наши внуки – в этих выродков Басава и Хаттаба”.

Отсутствие позитивного образа, без которого не обходится ни одно цивилизованное государство. Делает из преступников героев. Когда дети России будут играть в бойцов спецназа, вырывающих заложников из лап террористов, тогда российское общество окончательно выздоровеет, и опасная болезнь, грозившая уничтожить нашу страну, будет окончательно побеждена.