**Часть первая.**

Конфликт в Косово считается первой Интернет - войной. Правительственные и неправительственные лица одинаково стремились использовать сеть Интернет для распространения информации, ведения пропаганды, причинения вреда противнику, привлечения новых сторонников. Хакеры использовали сети для осуждения военных действий как Югославии, так и НАТО, путем нарушения работы правительственных компьютеров и получения контроля над сайтами. Индивидуумы рассказывали в Интернете истории об опасностях и ужасах войны, а политики и общественные деятели использовали всемирную паутину для того, чтобы их призывы достигли как можно более широкой аудитории. Люди всего мира обсуждали в сети спорные вопросы и обменивались текстами, изображениями и видео, которых нельзя было найти в иных средствах массовой информации. В апреле 1999 года газета *Los Angeles Times* написала, что Косовский конфликт превратил киберпространство в нематериальную военную зону, где сражение за умы и сердца ведется с помощью электронных изображений, групповых почтовых рассылок и хакерских нападений. Энтони Пратканис, профессор психологии Калифорнийского университета Санта Крус, отметил: “То, что вы видите сейчас – это только первая волна того, что очень скоро станет важным, высокоорганизованным инструментом в старой традиции пропаганды военного времени… это должно, если уже не принесло, то принести беспокойство военным стратегам”.

**Хактивизм** – это синтез социальной активности и хакерства. Под хакерством нами подразумевается эксплуатация компьютеров изощренными и часто незаконными способами с помощью специального (“хакерского”) программного обеспечения. Хактивизм включает в себя такие действия, как “электронное” гражданское неповиновение – использование методов гражданского неповиновения в киберпространстве. Мы исследуем четыре вида таких действий: виртуальные “сидячие забастовки” и блокады, бомбардировка электронной почты, web-хакерство и компьютерные взломы, компьютерные вирусы и черви. Поскольку подобные инциденты освещаются в СМИ, действия хактивистов и причины этих действий могут получить широкую огласку.

**Кибертерроризм**

В 1980-м году Бари Колин, старший исследователь Института Безопасности и Разведки в Калифорнии, вывел термин “кибертерроризм”, чтобы определить терроризм в киберпространстве. Специальный агент ФБР Марк Поллитт определяет кибертерроризм как “преднамеренные политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов”. Политически мотивированные атаки, причиняющие серьезный вред, типа серьезных экономических затруднений или длительных остановок энергоснабжения, водоснабжения, можно также охарактеризовать как кибертерроризм.

**Виртуальные “сидячие забастовки” и блокады.**

Виртуальная сидячая забастовка (демонстрация) или виртуальная блокада – это своеобразное “виртуальное” исполнение физической забастовки или блокады. В обоих случаях цель состоит в том, чтобы привлечь внимание к действиям протестующих и причинам этих действий, с помощью нарушения нормального функционирования сети и блокирования доступа к услугам.

При сидячей забастовке активисты посещают некий сайт и пытаются создать такой трафик, чтобы другие пользователи не смогли зайти на этот сайт. Первый протест такого рода осуществила группа, называющая себя “Strano Network”, протестовавшая против политики французского правительства в вопросах ядерных программ и социальной сфере. 21 декабря 1995 года эта группа в течение часа атаковала различные сайты правительственных агентств. Участники группы с разных континентов были проинструктированы следующим образом: им полагалось с помощью браузера зайти на правительственные сайты. По сообщениям, некоторые сайты действительно были выведены из строя на некоторое время.

В 1998 году группа под названием “Electronic Disturbance Theater” (EDT) сделала следующий шаг в развитии концепции электронного гражданского неповиновения. Ею был организован ряд забастовок в сети, сначала против сайта мексиканского Президента Зедильо, позже – против веб-сайта администрации Президента США Клинтона, сайтов Пентагона, Франкфуртской фондовой биржи, Мексиканской фондовой биржи. Цель данных демонстраций состояла в выражении солидарности мексиканцу Сапатитасу. По словам одного из деятелей EDT, Пентагон в качестве мишени был выбран потому, что “США воспитывает солдат для последующего нарушения прав человека”. Фондовые биржи были атакованы, поскольку, по мнению EDT, они выражают роль капитализма и глобализации, использующих методы геноцида и этнических “зачисток”, но народ должен выбирать свою судьбу сам, а не принудительно, под прицелом западного государства и западного финансирования.

Для проведения таких атак создаются специальные сайты, с которых скачивается автоматизированное программное обеспечение. Каждый участник должен посетить сайт, с которого загружается специальное программное обеспечение, которое запрашивает доступ к сайту-мишени каждые несколько секунд. Кроме того, это ПО позволяет протестующим производить иные операции – например, связанные с ошибками сервера. Например, если они направят браузер на несуществующий файл типа “права человека”, то сервер выдаст сообщение “права человека на этом сайте не найдены”.

В забастовке, проведенной EDT 9 сентября 1998 года (атака сайтов Президента Зедильо, Пентагона и Франкфуртской фондовой биржи), участвовало около 10000 человек со всех континентов, что составило 600000 попаданий в минуту на каждый сайт. Однако, Пентагон не сидел сложа руки. Был нанесен ответный удар. Когда на сервер Пентагона началась атака, одновременно было предпринято контрнаступление на браузеры пользователей, переориентировавшее их к странице с программой Applet (прикладная программа, запускаемая при каждом обращении к Web-странице, в исходный текст которой она встроена). Эта программа называлась “HostileApplet” (“Вражеская программа”). Программа загружалась в браузеры пользователей, что вызывало бесконечные требования перезагрузить документы, в результате чего перезагружались сами машины. Сайт Президента Зедильо не наносил ответного удара, но зато в качестве защиты было использовано программное обеспечение, заставившее браузеры протестующих открывать одно окно за другим, пока не “рухнет” компьютер. Франкфуртская фондовая биржа сообщила о том, что им было известно об атаке, но они полагают, что это никак не отразилось на их деятельности. По их словам, нормальная посещаемость сайта составляет 6 миллионов попаданий в день. В целом, EDT рассматривает свое нападение как успешное.

EDT использовал свое программное обеспечение “FloodNet” для атаки на сайт Белого дома, чтобы выразить протест экономическим санкциям США в отношении Ирака, а также выступая против военных ударов по Ираку. По заявлению EDT, участниками войны могут быть не только государства, киберпространство позволит вступать в конфликт также негосударственным политическим организациям и лицам, оно будет инструментом для оказания влияния на ход войны.

Активисты борьбы за права животных также использовали “FloodNet” для выражения протестов против жестокого обращения с животными. Более 800 человек из 12 стран присоединилось к акции протеста, проходившей в январе 1999 года и направленной против шведских сайтов.

Когда одновременно большое количество людей атакует сайт, как в случае с акциями протеста EDT, эти действия называют “роением” (“swarming”). Роение может использоваться для усиления эффекта от других нападений, например, e-mail бомбардировок.

Существует множество методов, при помощи которых лицо, действуя в одиночку, может нарушить или прекратить работу Интернет-серверов (в основном это DoS – инструменты). Белградские хакеры во время конфликта в Косово организовывали такие атаки против серверов НАТО. Они бомбардировали серверы командами, проверяющими, работает ли сервер и связан ли он с Интернетом. Ожидаемым эффектом таких атак была перегрузка линий сервера – мишени.

**Бомбардировка электронной почты.**

Одно дело послать одно - два письма политикам, пусть даже ежедневно. И совсем другое – бомбардировать их тысячами писем, отправленных одновременно при помощи автоматизированных инструментов. Это может привести к полной блокировке переполненного почтового ящика, делая невозможным получение электронной почты. Таким образом, бомбардировка электронной почты тоже является формой виртуальной блокады. Хотя бомбардировка электронной почты часто используется как средство мести или преследования, нередко использование этого инструмента для противодействия правительственной политике.

Первым известным нападением на почтовые ящики считается бомбардировка организацией “Тигры освобождения Тамила” электронных почтовых ящиков посольств Шри-Ланки, которые были завалены тысячами сообщений следующего содержания: “Мы Черные Тигры Интернет и мы делаем это, чтобы разрушить ваши коммуникации”. Одной из ветвей LTTE – Тамил Илам - приписывается бомбардировка электронной почты, произошедшая в 1998 году.

Эта бомбардировка состояла из приблизительно 800 писем в день в течение двух недель. Уильям Чурч, редактор центра CIWARS, отметил, что “Тигры освобождения Тамила отчаянно нуждаются в огласке, и они получили в точности то, что они хотели. Учитывая то, что террористическая деятельность этой организации заключается в кровавых терактах, этот тип деятельности гораздо более предпочтителен… CIWARS хотел бы поощрить их, от имени мира, отдавать большее предпочтение именно этому виду “террористических” действий”. Однако считается, что эта бомбардировка электронной почты была удачной, т. к. посеяла панику в посольствах.

Бомбардировке электронной почты в также подвергся в 1997 году основной поставщик Интернет – услуг в Сан-Франциско – Institute for Global Communications (IGC) за размещение на сайте *Euskal Herria Journal,* сомнительного издания Нью-Йоркской группы, поддерживающей независимость басков в Северной Испании и на Юго-западе Франции. Протестующие посчитали, что IGC “поддерживает терроризм”, поскольку на страницах сайта были материалы террористической группы “Родина и Свобода”, или ETA, ответственной за убийства более 800 человек за время тридцатилетней войны за независимость басков. Нападение против IGC началось после того, как члены ETA убили в Северной Испании популярного городского советника.

Целью протестующих была цензура. Они засыпали IGC тысячами подложных сообщений через сотни почтовых служб. В результате работа почты была парализована, и почту получить было невозможно, а линии поддержки были забиты людьми, которые не могли получить свою почту. Нападавшие также наводнили бесполезной информацией счета персонала и членов IGC, забивая их страницы поддельными заказами и номерами кредитных карт, и угрожали применить ту же тактику против организаций, пользующихся услугами IGC. Единственный способ, которым IGC мог остановить нападение – это блокировка доступа ко всем почтовым службам.

Сайт IGC закрылся 18 июля, однако перед закрытием зеркала этого сайта были размещены на нескольких сайтах на трех континентах. Крис Эллисон, представитель Кампании за свободу Интернет – английской группы, разместившей одно из зеркал сайта, сказал, что “сеть должна предоставлять возможность для обсуждения спорных идей”. Нью-Йоркский журнал настаивал на том, что его целью было “опубликование информации, часто игнорируемой международными СМИ, с целью лучшего понимания сути конфликта”. Французская газета Monde написала, что бомбардировка электронной почты IGCпредставляет собой “беспрецедентный конфликт”, открывший “новую эру цензуры, наложенной прямыми действиями анонимных хакеров”.

Через месяц после удаления IGC со своего сервера сайта журнала *Euskal Herria Journal* Антитеррористическое подразделение Скотланд-Ярда закрыло сайт английской Кампании за свободу Интернет, разместившей на сайте сомнительный журнал. Согласно официальному заявлению, эти действия были направлены на борьбу с терроризмом. Кампания за свободу Интернет заявила, что переместит журнал в свой Американский участок.

Случай с сайтом *Euskal Herria Journal* иллюстрирует мощь хактивистов в Интернете. Несмотря на свое желание, IGC не смог оставить сайт на своем хостинге, поскольку мог не выдержать нападения. Можно было бы проигнорировать несколько сообщений электронной почты, требующих закрыть сайт, но нельзя игнорировать бомбежку электронной почты. Случай также иллюстрирует мощь Интернет как средства свободы слова.

**Web-хакерство и компьютерные взломы**

Средства массовой информации заполнены историями о хакерах, получающих доступ к сайтам, и меняющих содержание страниц. Часто сообщения связаны с политикой – как, например, сообщение о том, что группа португальских хакеров изменила в сентябре 1998 г. содержание 40 индонезийских сайтов, разместив на них большими черными буквами слоган “Свобода Восточному Тимору”. По сообщениям *New York Time*s, хакеры также добавили ссылки на сайты, размещающие информацию о нарушении Индонезией прав человека в бывшей португальской колонии. Тогда, в августе 1999 года, Нобелевский лауреат Хосе Рамон Хорта, представляющий движение за независимость Восточного Тимора от Индонезии, предупредил о существовании плана глобальной сети хакеров на случай, если Джакарта сорвет голосование о будущем Восточного Тимора. В заявлении, сделанном *Sydney Morning Herald*, он сказал, что план готовили более 100 хакеров, в основном подростков, из разных стран.

В июне 1998 года, международная группа хакеров, называющая себя Milw0rm, получила доступ к Индийскому центру атомных исследований Bhabha Atomic Research Center (BARC) и создал фальшивую страницу сайта с ядерным грибом и надписью: “Если начнется ядерная война, вы закричите первыми…” Хакеры протестовали против испытаний ядерного оружия, проведенных в Индии, хотя некоторые признавали, что сделали это главным образом в поисках острых ощущений. Они также заявили, что скачали несколько тысяч страниц электронной почты и исследовательских документов, включая переписку между учеными-атомщиками Индии и должностными лицами израильского правительства, и уничтожили данные на двух серверах BARC. Все это было сделано шестью хакерами из США, Англии, Нидерландов и Новой Зеландии, возрастной диапазон которых – от 15 до 18 лет.

Другой путь, которым хактивисты изменяют информацию, просматриваемую пользователями – это вмешательство в работу службы доменных имен, так, чтобы название одного сайта, приводило на IP другого. Когда пользователи направляют браузеры на один сайт, их переадресовывают к альтернативному.

Самой большой акцией подобного рода была совместная атака более трехсот сайтов антиядерными хакерами Milw0rm совместно с хакерами группы Ashtray Lumber-jacks в июле 1998 года. По сообщениям, хакеры получили незаконный доступ сайтам Британского провайдера EasySpace. Они изменили базу данных провайдера так, что все пользователи, пытавшиеся получить доступ к сайтам, попадали на сайт с лозунгом протеста против гонки вооружении: “используй свою силу для поддержания МИРА и положи конец этому ядерному абсурду”.

После случайной бомбежки силами НАТО китайского посольства в Белграде, рассерженные китайские хакеры взломали несколько американских правительственных сайтов. На сайте американского посольства в Пекине был помещен лозунг, в котором американцы назывались варварами, в то время как на сайте Департамента внутренних дел были размещены фотографии трех журналистов, убитых во время бомбежки, пекинских демонстраций против войны, и изображение китайского флага. Согласно *Washington Post*, представитель Департамента внутренних дел США Тим Ахеарн заявил, что экспертам удалось найти след хакеров, ведущий в Китай. Газета также сообщила о заявлении, размещенном на сайте Министерства энергетики США:

*“Протестуем против нацистских действий США! Дайте отпор бесчеловечным деяниям! Мы – китайские хакеры, не заботящиеся о политике. Но мы не можем оставаться спокойными, видя наших китайских репортеров убитыми – вы знаете кем. Независимо от цели, НАТО во главе с США должно нести полную ответственность. Вы в кровавом долгу перед китайским народом, и вы должны оплатить этот долг. Мы не прекратим атак, пока вы не прекратите войну!”*

НАТО, конечно, не прекратило войну из-за этих атак. Бомбежка сама по себе повлияла на внешнюю политику неизмеримо сильнее, чем эти атаки (если они вообще повлияли). После несчастного случая Китай приостановил военные контакты с США на высшем уровне.

*Los Angeles Times* сообщили, что калифорнийский студент факультета информатики, называющий себя Бронк Бастер, со своим компаньоном Зайклоном, взломал китайскую сеть и стер управляемый государством сайт по правам человека и цензуре. По словам хакера, они обнаружили примерно 20 серверов firewall, блокирующих все от Playboy.com до Parents.com. Никакие данные не уничтожались, их лишь переместили.

Бронк Бастер принадлежал к группе 24 хакеров, известной как Legion of the Underground (LoU) – Легион Подполья. На пресс-конференции в чате IRC в конце декабря 1998 года один из членов LoU объявил кибервойну информационным структурам Китая и Ирака. Он привел примеры нарушения гражданских прав и призвал к разрушению всех компьютерных систем Китая и Ирака.

Объявление кибервойны побудило коалицию из других хакерских групп выступить против этой кампании. Письмо, подписанное хакерскими группами Chaos Сomputer Club, the Cult of the Dead Cow (CDC), !Hispahak, L0pht Heavy Industries, Phrack, Pulhas, и некоторыми группами Нидерландского сообщества хакеров, осудило кибервойну. По их заявлению, “объявление войны стране – самый безответственный поступок, который может совершить группа хакеров. Это не имеет никакого отношения к хактивизму или хакерской этике, и содержит ничего, чем хакер может гордиться”. Представитель CDC Рейд Флеминг сказал, что “никто не может улучшить свободный доступ нации к информации путем нарушения работы сетей и уничтожения данных”.

К тому времени, как появилось это письмо, объединение LoU уже заявила, что объявление войны в IRC не выражало позицию группы. “LoU не поддерживает заявление о повреждении компьютеров, сетей или систем других наций, при этом LoU не будет использовать свои способности, навыки, связи для проведения любых действий против компьютеров, систем или сетей в Китае или в Ираке, могущих повредить их или препятствовать каким-либо образом их деятельности”. Бронк Бастер сказал, что член группы, продекларировавший войну, выбыл из группы и никогда не вернется обратно.

**Компьютерные вирусы или черви.**

Компьютерные вирусы или черви используются хактивистами для распространения лозунгов протеста или повреждения компьютерных систем. Обе формы поражают компьютер и распространяются по компьютерным сетям. Граница между ними является расплывчатой, и мы не будем обсуждать их отличия друг от друга, поскольку для нашего исследования эти отличия не важны.

Первый протест, связанный с использованием червя, прошел больше десяти лет назад, когда хакеры, протестующие против ядерной войны, запустили червя в сеть Администрацию национальной аэронавтики и космонавтики США. 16 октября 1989 г. ученые увидели на компьютерах центра управления полетами НАСА в Гринбелт, штате Мериленд, приветствие со знаменем червя WANK: “Черви против ядерных убийц. Вы говорите о времени мира для всех, а потом готовитесь к войне”.

Во время нападения протестующие пробовали остановить запуск космического челнока, который нес оборудование, питающееся от радиоактивного плутония, на Юпитер. Джон Макмахон, менеджер НАСА, оценил потери, которые принес червь, как полмиллиона долларов потраченных впустую времени и ресурсов. Хакеры не добились остановки запуска. Источник нападения не был идентифицирован, но есть предположения, что это были австралийские хакеры.

Компьютерные вирусы использовались для распространения политических заявлений, и в некоторых случаях повлекли серьезный ущерб. В феврале 1999 года *London Sunday Telegraph* сообщила, что израильский подросток, заявивший о том, что им уничтожен иракский правительственный сайт, стал национальным героем. “Сайт содержал ложь о США, Великобритании и Израиле, а также множество ужасных заявлений против евреев”, - сказал четырнадцатилетний Нир Зигдон. – “Я полагал, что если Израиль боится убить Саддама Хусейна, то я могу, по крайней мере, уничтожить его сайт. С помощью специального программного обеспечения я выследил сервер сайта в одной из стран Персидского залива”. Тель-Авивский хактивист послал на сайт компьютерный вирус в приложении к электронной почте. “В письме я написал, что я являюсь палестинским поклонником Саддама и мною создан вирус, способный уничтожить израильские сайты. Это убедило их открыть вложение. В течение часа сайт был уничтожен. Вскоре я получил электронную почту от менеджера сайта, который велел мне ‘идти к черту’”.

Вирусы, особенно разрушительные, являются потенциально мощным инструментом в руках кибертеррористов. Другие инструменты хактивизма, включая нападения на компьютерные сети, могут также быть использованы в разрушительных целях.