

Интернет - инструмент политики

Т.е. инструмент достижения политических целей:

- **Локальное применение:** завоевание и удержание власти в своей стране.
- **Глобальное противостояние:** интернет как рычаг силы - давление на противника, на его эллектрорат.

Генри Киссинджер назвал это это глобальной шахматной партией (найдите почитайте - это классика - ее нужно знать). Однако это не игра. Это очень серьёзно.

Данный текст — компиляция цитат (ссылки и авторы приводятся) и моих размышлений на тему, - подготовлен как материалы к лекции для студентов 1 курса МО МГИМО.

Собрал вместе Александр Немченко

23 марта 2017 г.

г. Москва

А начиналось все просто сказочно.



<http://rvb.ru/pushkin/01text/03fables/01fables/0799.htm>

А. С. Пушкин СКАЗКА О РЫБАКЕ И РЫБКЕ

Жил старик со своею старухой
У самого синего моря;
Они жили в ветхой землянке
Ровно тридцать лет и три года.
Старик ловил неводом рыбу,
Старуха пряла свою пряжу.

Раз он в море закинул невод,
Пришел невод с одною тиною.
Он в другой раз закинул невод,
Пришел невод с травой морской.
В третий раз закинул он невод,
Пришел невод с одною рыбкой,
С непростой рыбкой, - золотую.

Вот идет он к синему морю,
Видит, на море черная буря:
Так и вздулись сердитые волны,
Так и ходят, так воем и воеют.
Стал он кликать золотую рыбку.
Приплыла к нему рыбка, спросила:
"Чего тебе надобно, старче?"
Ей старик с поклоном отвечает:
"Смилуйся, государыня рыбка!
Что мне делать с проклятою бабой?
Уж не хочет быть она царицей,
Хочет быть владычицей морской;
Чтобы жить ей в Окияне-море,
Чтобы ты сама ей служила
И была бы у ней на посылках".

Ничего не сказала рыбка,
Лишь хвостом по воде плеснула
И ушла в глубокое море.
Долго у моря ждал он ответа,
Не дождался, к старухе воротился
Глядь: опять перед ним землянка;
На пороге сидит его старуха,
А пред нею разбитое корыто.

Сказка ложь, да в ней намек - добрым молодцам урок!

DARPA

https://ru.wikipedia.org/wiki/Управление_перспективных_исследовательских_проектов_Министерства_обороны_США

Управление перспективных исследовательских проектов Министерства обороны США
DARPA - Defense Advanced Research Projects Agency

Основано в 1958 году в ответ на запуск в СССР первого искусственного спутника Земли. Перед DARPA была поставлена задача сохранения превосходства военных технологий США.

DARPA существует независимо от обычных военных научно-исследовательских учреждений и подчиняется непосредственно руководству Министерства обороны.

Штат DARPA насчитывает около 240 сотрудников (из которых примерно 140 — технические специалисты); бюджет организации составляет около 3 миллиардов долларов.

ARPANET (от англ. Advanced Research Projects Agency Network) — компьютерная сеть, созданная в 1969 году в США Агентством Министерства обороны США по перспективным исследованиям (DARPA) и явившаяся прототипом сети Интернет. 1 января 1983 года она стала первой в мире сетью, перешедшей на маршрутизацию пакетов данных. В качестве маршрутизируемого протокола использовался IP, который и по сей день является основным протоколом передачи данных в сети Интернет. ARPANET прекратила своё существование в июне 1990 года.

В декабре 2009 года DARPA запускало красные шары-метеозонды в небо США, чтобы проверить возможности сбора, анализа и обмена информацией с помощью социальных сетей. Все 10 шаров были найдены менее чем за 9 часов[6], призовой фонд проекта составил 40 000 долларов.

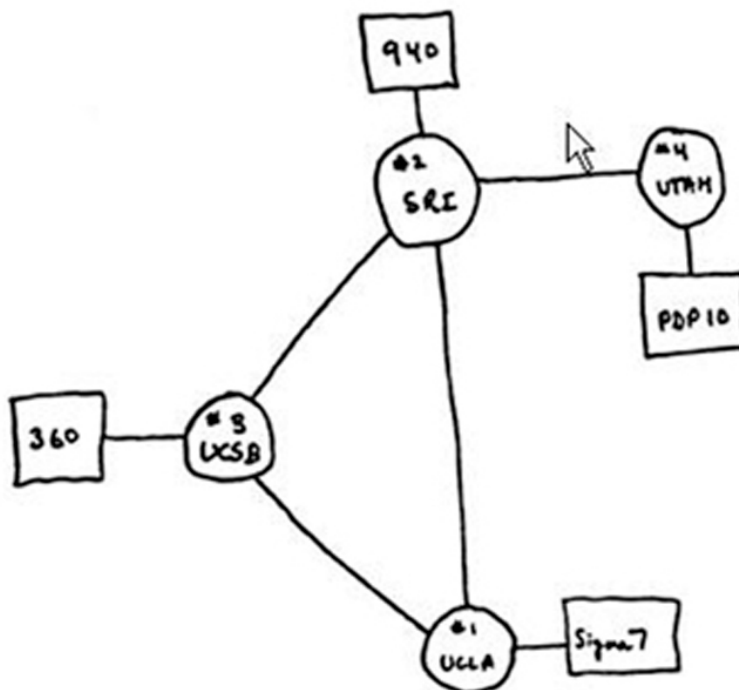
Осенью 2014 года стало известно о завершении разработки революционного процессора Terahertz Monolithic Integrated Circuit (TMIC) способного работать на тактовой частоте 1 ТГц[7][8]. Этот результат стал рекордным на момент выхода процессора. Примечательно, что предыдущий рекорд производительности был так же установлен DARPA в 2012 году. В сентябре 2015 года представитель DARPA заявил, что несколько десятков людей, которым вживили разрабатываемые агентством искусственные имплантаты, дающие направленные электрические разряды в определённые доли мозга, показали значительные улучшения в тестах на проверку памяти. Согласно предварительным результатам исследователи смогли не только записать и интерпретировать сигналы, сохраняющие воспоминания, но и улучшить способность пациентов запоминать целые списки объектов.

<http://devicebox.ru/internet-history/>

К слову, первый сервер сети ARPANET был запущен 2 сентября 1969 года в Калифорнийском университете города Лос-Анджелес. Это был к Honeywell DP-516 с оперативной памятью всего 24 Кб. А уже 29 октября 1969 года в 21 час по местному времени между двумя первыми узлами сети ARPANET, расположенными на удалении 640 километров друг от друга — в Калифорнийском университете (UCLA) и Стэнфордском исследовательском институте (SRI) — бы проведен первый сеанс связи. Ученый Чарли Клайн (Charley Kline) смог тогда подключиться к компьютеру в SRI и передать всего три символа «LOG» до того, как сеть перестала работать. Он хотел написать слово LOGON (команда для входа в систему), но не

успел. Систему практически сразу же вернули в рабочее состояние и их следующая попытка увенчалась успехом. Некоторые источники именно 29 октября считают Днём Рождения Интернета, хотя фигурируют и другие даты.

**Набросок схемы соединения первых
четырёх узлов ARPANET в конце 1969 г.
Квадраты - компьютеры с указанием
модели, окружности - процессоры сообщений с
указанием места установки**



В 1971 году было разработано первое приложение для отправки электронной почты (e-mail), и оно сразу стало очень популярным. Тогда же, в 70-х годах сеть использовалась в основном только для рассылки электронной почты. Начиная с января 1983 года сеть ARPANET сменила протокол с NCP на TCP/IP. Этот протокол успешно применяется для объединения сетей и в наши дни. И именно тогда, в 1983 году за сетью ARPANET закрепился термин «Интернет».

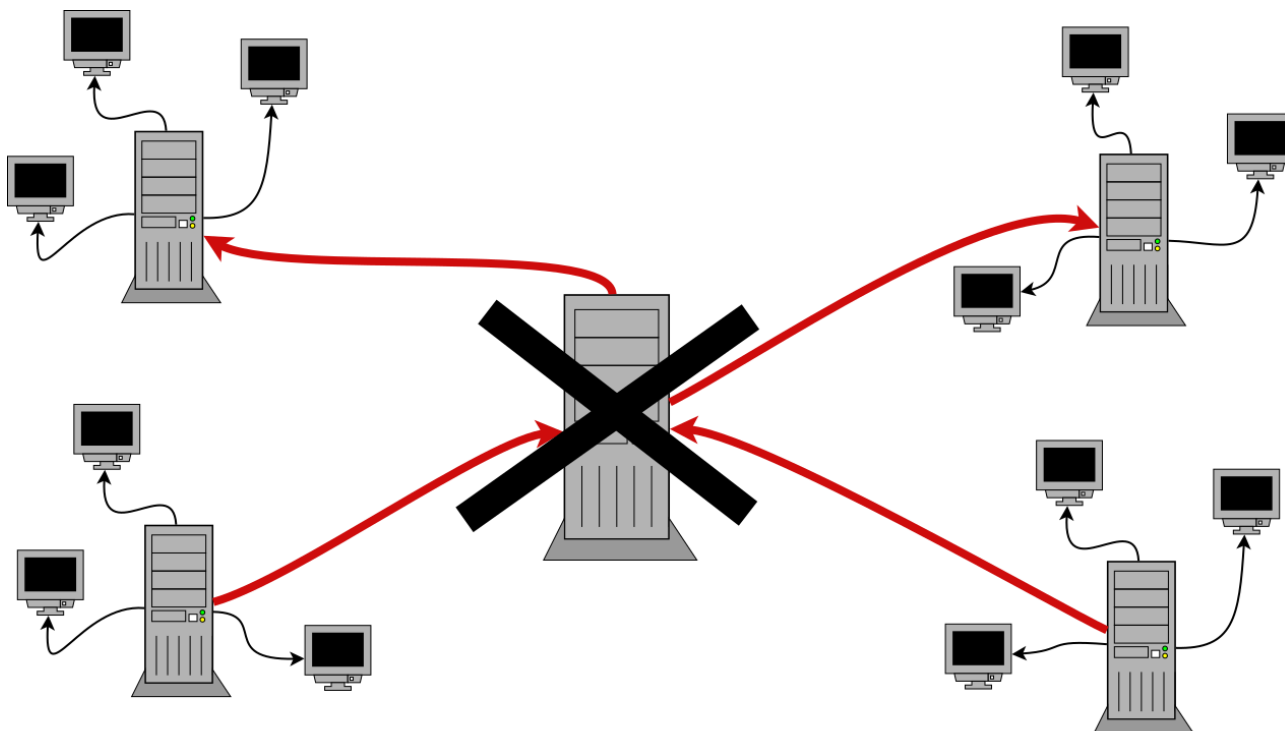
В 1991 году паутина стала общедоступной, а для удобства работы с ней программисты создали большое количество приложений и софта. В 1993 году был выпущен первый браузер NCSA Mosaic, который обладал графическим интерфейсом и был достаточно простым в использовании.

http://www.aif.ru/dontknows/file/chto_takoe_voennoy_internet

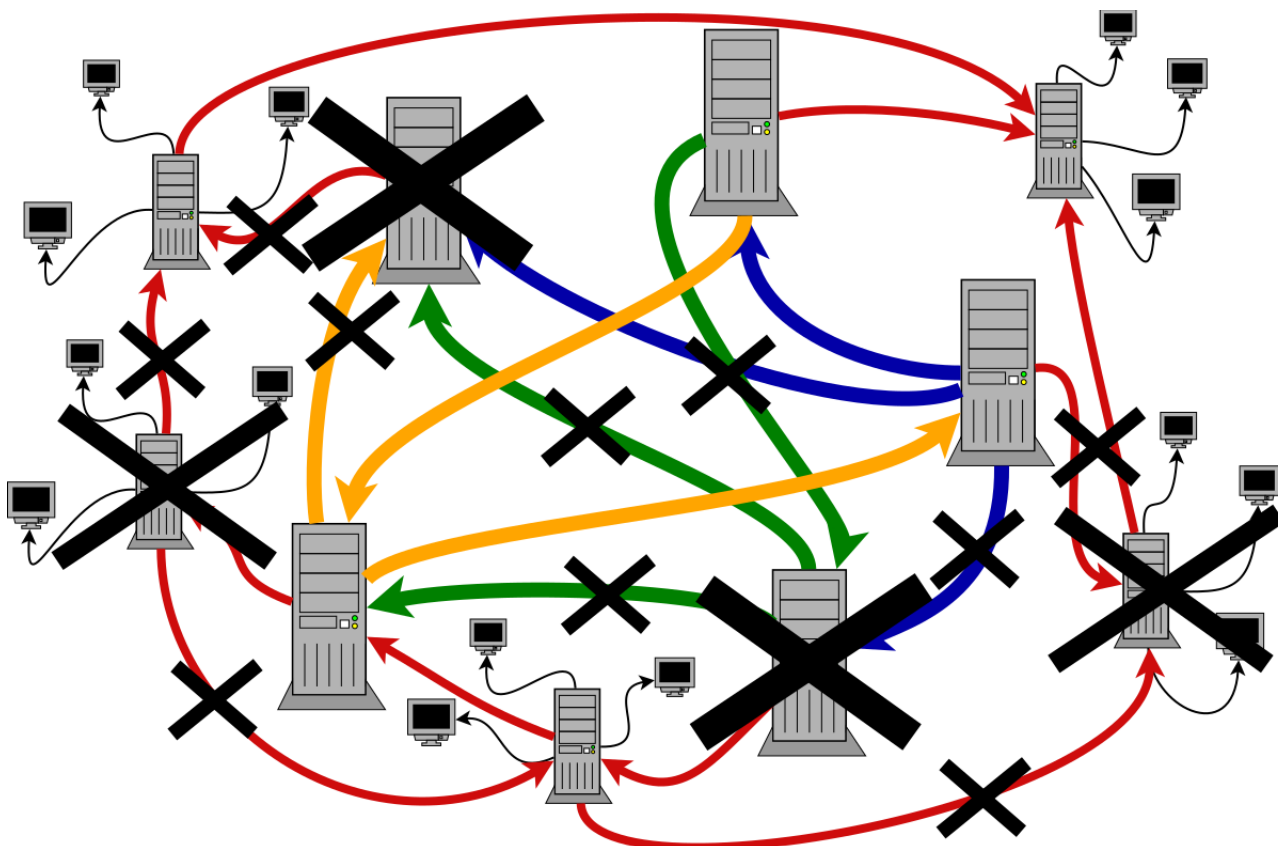
Такая глобальная военная сеть существует не только в российской армии. Наше нововведение по масштабу сравнимо с закрытой сетью, действующей в вооружённых силах США. Военный интернет создан также и в Израиле, над такой сетью работает Китай.

<https://www.youtube.com/watch?v=MbMAPoga8tE> - Ролик "История Интернета" - 8 мин.

Уязвимая сеть передачи данных



Неуязвимая сеть передачи данных



Социальные параметры интернета

<http://www.shapovalov.org/publ/7-1-0-89>

1. Для широкого распространения информации он не требует от потребителя сети высоких материальных затрат, что позволяет использовать этот источник массовой информации небогатым слоям населения, причем как небогатым получателям информации, так и небогатым авторам информации. Последнее наиболее важно, ибо от личной позиции автора информации и зависит в первую очередь характер информации, правдивая эта информация или ложная. Технология и организация традиционных СМИ (печатные СМИ, радио и телевидение) такова, что позволяет отсеять редакциям неугодных авторов на самом начальном этапе производства информационного продукта. Сам автор или даже группа авторов изготовить самостоятельно информационный продукт методами традиционных СМИ тоже не в состоянии, слишком уж велики материальные издержки на его производство и распространение.
2. Способность интернета почти мгновенно оповещать огромное количество потребителей, в чем интернет на сегодня практически вплотную приближается к телевидению и, скорее всего, в самое ближайшее время даже намного его превзойдет в массовости.
3. Скорость поступления информации потребителю (оперативность) – здесь интернет вообще вне конкуренции, особенно после того, как массе населения стали доступны технологии, позволяющие передавать информацию через мобильные телефоны.
4. Сложность организовать цензуру и хоть как-то отслеживать и контролировать поступающую в интернет информацию. Т.е. на сегодня это действительно наиболее свободные средства массовой информации.
5. Наличие обратной связи, т.е. возможность потребителей информации тут же высказать свое мнение относительно того или иного информационного продукта, что позволяет автору мгновенно среагировать и быстро скорректировать свой информационный продукт в нужном русле - качество, которым обладает на сегодня только интернет.
6. Доступность информационного продукта любому пользователю в любое время. Возможность многократного использования информационного продукта. Замечательная особенность, присущая только интернету.
7. Единое мировое информационное пространство, в котором нет ни границ, ни таможен, ни даже расстояний. Уникальная особенность интернета.

Кибервойна

<http://vpoanalytics.com/2014/06/27/internet-kak-sredstvo-dostizheniya-voennyx-i-politicheskix-celej/>

Дмитрий Литвинов, Александр Крикунов «Центр анализа террористических угроз»

В настоящее время сеть Интернет все активнее и масштабнее используется в интересах информационного противоборства сторон, являющихся участниками различных конфликтов. Она предоставляет широкие возможности в плане оказания влияния на формирование общественного мнения, принятие политических, экономических и военных решений, воздействия на информационные ресурсы противника и распространение специально подготовленной информации (дезинформации).

При этом необходимо различать два направления ведения информационного противоборства: непосредственно информационное и психологическое. В первом случае объектом воздействия становятся компьютеры и информационные системы, во втором — индивидуальное и массовое сознание.

В случае проведения психологической войны на первое место выходят процессы формирования общественного мнения. В этом случае эффективно воздействует преуменьшение значимости того или иного события, недопущение его в информационное пространство, использование, так называемой, «спирали молчания», то есть представления мнения меньшинства, как мнения большинства населения и смещение, таким образом, смысловых и идеологических акцентов.

В рамках информационно-психологических операций действия сил и средств могут быть направлены на:

- реструктурирование враждебных отношений избранных индивидов и групп;
- усиление отношений дружески настроенных индивидов и групп;
- поддержание постоянной нейтрализации тех, чьи отношения являются неструктурированными, кто является «безопасным», будучи нейтральным.
- Кроме психологической составляющей информационного противоборства в ходе глобальной информатизации существенное влияние оказывает и техническая составляющая, которая формирует принципиально новую среду противоборства конкурирующих государств — киберпространство.

Если в мире к настоящему времени сложился в той или иной степени стратегический баланс сил в области обычных вооружений и оружия массового уничтожения, то вопрос о паритете в киберпространстве остается открытым.

В процессе формирования киберпространства происходит сближение военных и гражданских компьютерных систем и технологий. Государственные органы все шире закупают для решения военных и других специальных задач аппаратно-программные средства, разработанные коммерческими производителями для широкого круга пользователей.

Растет также потребность в совместимости гражданской информационной инфраструктуры с

правительственной и военной. В связи с этим происходит их технологическое и организационное слияние. Так, 95% линий связи компьютерных сетей Министерства обороны США развернуто на базе общедоступных телефонных каналов, а свыше 150 тыс. компьютеров подключены к сети Интернет, что делает их чрезвычайно уязвимыми.

Весь стандартизированный компьютерный комплекс может быть быстро выведен из строя применением одного конкретного средства, атакой, ориентированной на общий для стандартизированной сети уязвимый элемент — например, операционную систему или протокол связи.

По мнению западных аналитиков, ЦРУ, АНБ и военная разведка США активно изучают возможности и методы проникновения в компьютерные сети своих потенциальных противников. Для этого, в частности, разрабатываются технологии внедрения электронных вирусов и «логических бомб», которые, не проявляя себя в обычное время, способны активизироваться по команде.

В кризисной ситуации «электронные диверсанты» могут дезорганизовать оборонную систему управления, транспорт, энергетику, финансовую систему другого государства. Перспективными для таких целей считаются «заражённые» микросхемы, внедряемые в экспортируемую Соединёнными Штатами вычислительную технику.

Способы использования Сети Интернет в целях влияния на военные и политические решения.

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.

Для проведения 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».

Распространение специально подобранной информации (дезинформации). Оно осуществляется путем рассылки электронных писем e-mail, организации новостных групп, создания сайтов для обмена мнениями, размещения информации на отдельных страницах или в электронных версиях периодических изданий и сетевого вещания (трансляции передач радио- и телестанций).

Web-хакерство и компьютерные взломы. Наиболее распространенным направлением использования глобальной сети в интересах вышеупомянутого противоборства является замена информационного содержания сайтов, заключающаяся в подмене страниц или их отдельных элементов в результате взлома. Такие действия предпринимаются в основном для привлечения внимания к атакующей стороне, демонстрации своих возможностей или являются способом выражения определенной политической позиции. Помимо прямой

подмены страниц широко используется регистрация в поисковых системах сайтов противоположного содержания по одинаковым ключевым словам, а также перенаправление (подмена) ссылок на другой адрес, что приводит к открытию специально подготовленных противостоящей стороной страниц.

Особо следует выделить так называемые семантические атаки, заключающиеся во взломе страниц и последующем аккуратном (без заметных следов взлома) размещении на них заведомо ложной информации. Подобным атакам, как правило, подвергаются наиболее часто посещаемые информационные страницы, содержанию которых пользователи полностью доверяют.

Вывод из строя или снижение эффективности функционирования структурных элементов сети путем применения специальных программных и аппаратно-программных средств на основе программного кода: программные и аппаратные закладки, компьютерные вирусы, «сетевые черви» и т. п.

Опыт Франции в этом вопросе

Информационное противоборство в информационно-телекоммуникационных сетях рассматривается французскими военными как универсальное средство, позволяющее решать широкий спектр задач — от деструктивного воздействия на компьютерные системы и сети противника до получения разведывательных сведений стратегического характера в интересах национальной обороны и обеспечения успеха боевых действий.

Принципами организации информационно-технического противоборства являются: непрерывность; единство управления; адекватность угрозам; унификация правил применения сил и средств; обеспечение квалифицированными кадрами.

Французские эксперты выделяют три фазы проведения операций в киберпространстве:

подготовительный этап, в ходе которого основные усилия сосредотачиваются на сборе информации о противнике;

собственно воздействие на неприятеля;

обеспечение безопасности своего информационного пространства.

В соответствии с проектом концепции мероприятия должны осуществляться по следующему алгоритму:

Обоснование целесообразности и принятие решения о его проведении. Для этого собирается информация о компьютерных системах и телекоммуникационных сетях противника. Кроме того, обобщаются сведения о собственном наступательном и оборонительном потенциале. Обеспечение превосходства над противником в информационной сфере путем получения доступа к данным, циркулирующим в автоматизированных информационных системах противника. Актуализация возможностей и намерений неприятеля, идентификация вероятных объектов атаки.

Деструктивное воздействие на информационную инфраструктуру неприятеля: дезорганизация работы отдельных компьютеров и их сетей; снижение пропускной способности информационно-телекоммуникационных сетей и ухудшение функционирования систем управления оружием. Одновременно рекомендуется проводить мероприятия по защите собственных информационных систем от подобных акций противника. Использование превосходства в киберпространстве для осуществления информационно-психологического воздействия на противника (введение в заблуждение, подрыв моральных и

волевых качеств, нарушение процесса принятия решений, разрыв иерархических и функциональных связей в системе управления).

Таким образом, глобальная сеть Интернет сегодня играет огромную роль в глобализации информационных войн и является эффективным средством воздействия на информационные ресурсы своих соперников и военно-политическое руководство противоборствующих сторон при принятии ими важных решений.

При этом следует отметить, что на заседании комитета начальников штабов блока НАТО в 2011 году было принято решение о приравнивании кибератак на информационные ресурсы стран участниц блока к военной агрессии. Что подчёркивает важность киберпространства и его решающее значение в современном информационном противоборстве.

ГИС Интернет является одним из эффективных средств достижения военных и политических целей между противоборствующими государствами и их коалициями. Что активно используется соперниками в информационных войнах.