Интернет "для диссидентов"

Когда бюрократам надо выбить финансирование на различные технические новации, они обращаются к обычным ИТшникам, чтобы те помогли им объяснить старые технологии с помощью новых слов. Именно так, к примеру, родился термин "теневой интернет", который пару месяцев назад встряхнул глобальную сеть в помощью "разоблачений" и обещаний правительства США дать возможность "повстанцам", а также "борцам за свободу" подключаться к Сети даже при тотальном контроле за магистральными каналами связи со стороны многих "тоталитарных правительств". Ведь организация и управления мобильными группами "граждан" любой направленности осуществляется с помощью мобильных систем связи. Поэтому - рассмотрим на практике чем эта "технология" или уже, скорее, бренд, будет полезен для обычных пользователей и операторов связи.

"Неубиваемые" сети

Если вспомнить совсем недалекую историю, то можно отметить, как несколько лет назад в США отмечался бум беспроводных сетей в сегменте "общественной безопасности". Муниципалитеты всех уровней были готовы использовать для этого мобильный WiMAX (тогда это считалось передовой технологией мобильной широкополоски - мир еще не "подсел на LTE), который обеспечивал высокую скорость и высокую "живучесть" подобных сетей. Эти проекты "товарищами в погонах" были внимательно изучены и что-то нашло применение в военных системах. Для гражданских же нужд были предложены различные варианты Mesh-сетей, которые бы работали как на основе Wi-Fi, так и Bluetooth или EDGE/HSPA. LTE – в перспективе тоже рассматривается.



«Неверных не видно? Сейчас запостим фотки на Facebook!»

Основное отличие таких сетей от всех остальных гражданских аналогов - полноценная децентрализация и «самоорганизация» (в кавычках потому, что управление происходит в полуавтоматическом режиме). Но в идеале сеть, даже будучи микромиром "сам-в-себе" может выстраивать наиболее адаптивную конфигурацию работы в зависимости от того, какой ее сегмент "выбивается", к примеру, стихийными бедствиями или организационными мерами властей. В самой простой ситуации принцип работы таких систем можно описать как "все-со-всеми": каждая базовая станция одновременно обслуживает пользователей и является магистральным сегментом сети, передающем информацию от соседей внутри системы связи. Если какое-то количество транспортных узлов (на самом деле "узел" - слишком громкое название, в его роли может выступать обычный роутер) выходит из строя, их абонентов и транспортные каналы автоматически "подхватывают" другие базовые станции.



В странах с несколько нестабильной инфраструктурой связи необходимы дублирующие решения

Отмечу, что Mesh-сетки строить не так уж и сложно – если поискать, можно найти десятки примеров за весьма скромные деньги с различной типологией такой сети и различным оборудованием. Кто-то даже считает, что самым большим примером такой системы можно считать проект Beeline Wi-Fi в Москве, который построен на оборудовании Nortel. Но, на мой взгляд, это больше показуха, чем реально полезно решение, которое приносит своему владельцу прибыль.

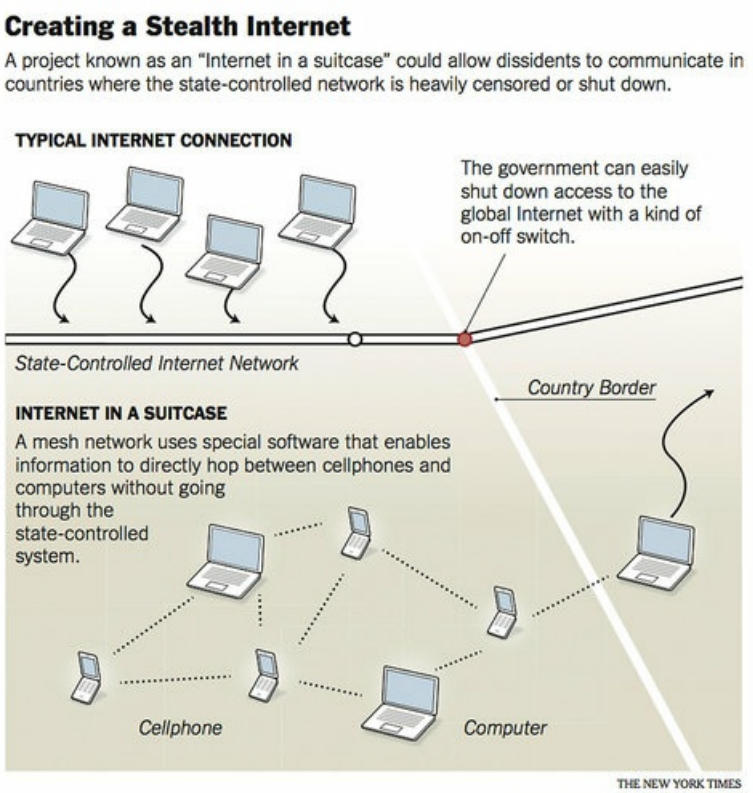


Схема «теневого интернета»: если нельзя подключиться легально, надо это сделать нелегально – добить радиосигналом через границу, к примеру.

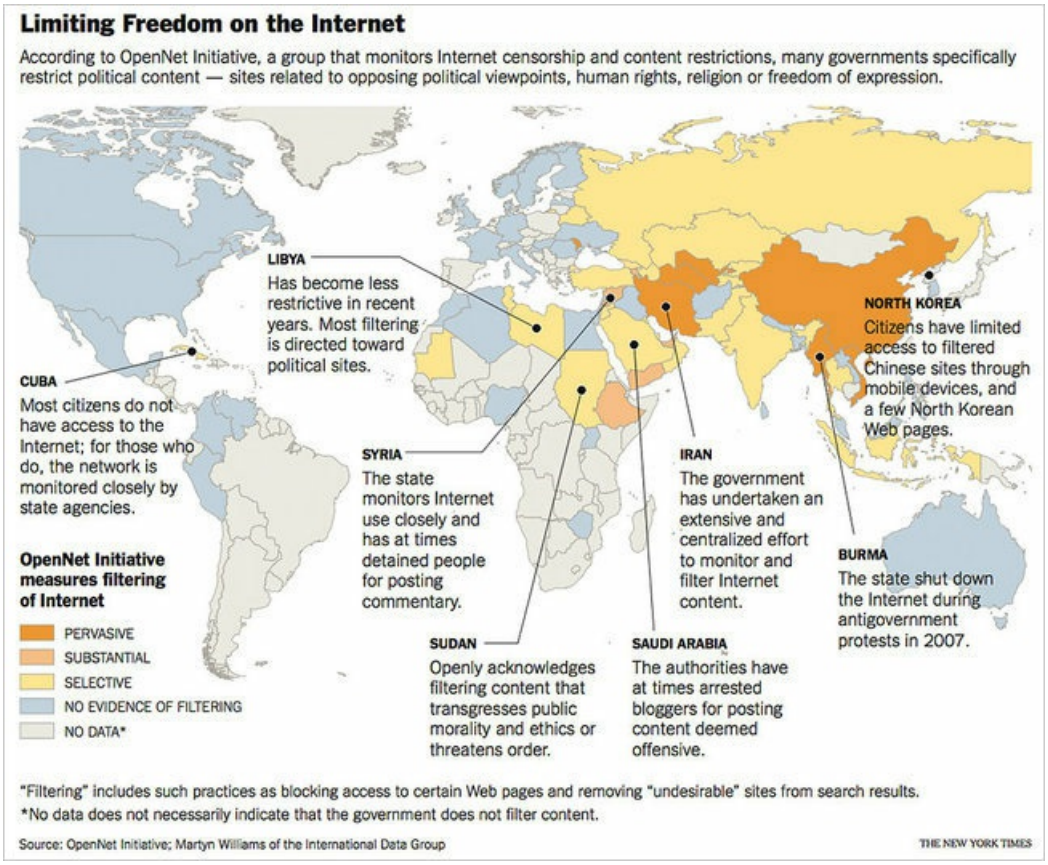
В любом случае, не вызывает никакого сомнения то, что "теневой интернет" - это технологическая игрушка, применяемая для ведения психологической войны. Как бы странно/страшно или смешно не звучали такие термины, но это соответствует новой реальности, в которой «пользовательский контент», поданный даже «без купюр», но с соответствующими «приправами» в виде контекста передачи, пользуется бешеным успехом. Вспомним, что съемка на камеру мобильного телефона с дрожащих рук, размещенная на YouTube через несколько минут после того или иного события, будет восприниматься, для огромного числа людей, куда как более очевидно и серьезно, вызывать гораздо большее доверия, чем репортаж любого официального или "независимого" ТВ-канала. Эти самые каналы даже используют такую «нарезку видеокадров» как иллюстрации к своим репортам: не брезгует этим ни CNN ни Euronews. Что уж говорить о нашем «любимом» LifeNews. А ведь для того, чтобы можно было передать такие ролики из гущи событий, чтобы можно было дать возможность

отправлять сообщения в социальные сети, проекты "теневого интернета" и развиваются.



Даже древних железок XO-1 проекта One Laptop Per Child вполне хватает для отправки записей в Сеть

Причем, задача мобильных комплексов связи в проектах "теневого интенета" - не передача секретной разведывательной информации. Кому она нужна. :) Во всяком случае, не таким образом. Их основная задача - создать автономную, по возможности мобильную инфраструктуру для выхода в Сеть по беспроводным каналам связи. Причем организовать значительную часть этой самой инфраструктуры из подручных материалов или недорогого оборудования, которое можно быстро заменить. Поэтому какой-то типовой схемы сборки подобных систем нет - все очень динамично и зависит от необходимой силы сигнала, от того на какой частоте будут общаться друг с другом устройства, а также от местности, где будет разворачиваться такая система. Для ее управления достаточен легкий, простой и недорогой нетбук, роутер/хаб/маршрутизатор, антенны (направленные или круговые), а также комплекс связи с той системой, которая даст возможность подключить это все к сети Интернет: чаще всего это сотовая связь или проводное подключение или, реже всего из-за своей дороговизны, спутниковый модем.



В этих страна, по мнению Госдепа США, есть «проблемы с доступом к информации» со стороны

самых обычных людей. Значит им показан «теневой интернет».

Кстати, в том же госдепе США совсем не скрывают того факта, что новые технологии в первую очередь предназначены для "гражданских активистов" в Иране, Сирии и Ливии. В списке стран, ограничивающих свободу информации, упоминается и Россия, где, по мнению Вашингтона, применяется "избирательная цензура". :) Дело в том, что локальные чиновники «от связи» многих стран достаточно быстро поняли: для препятствия выхода информации, к примеру, о столкновениях народа с армией или полицией в Сеть, надо оперативно блокировать фиксированные и мобильные каналы связи. Однако, с помощью мобильных комплексов, которые сложно отследить и практически невозможно "заглушить", эта проблема может быть решена. Тем более она не может быть решена, если организаторы таких систем обладают спутниковой связью или могут «прицепится» к сотовым «вышкам» от провайдеров, которые можно поймать на границе государства.

Подключение без цензуры

Активности спецслужб США можно только позавидовать - ведь они творчески используют те технологические наработки, которые реализовывались достаточно давно. Просто приспособили уже имеющееся оборудование для своих нужд, получили дополнительное финансирование под красивый «бизнес-план» и, самое главное, могут продемонстрировать что-то работающее для соответствующих комиссий Конгресса. Российские «коллеги» именно в умении устраивать шоу и, заодно, получать какой-то позитивный результат заокеанским представителям спецслужб, конечно, уступают.

При том, что сама по себе задача быстрого построения и типовой, практически мгновенной настройки локальных беспроводных сетей пользователями, которые слабо разбираются в информационных технологиях - вполне решаема. Над этой проблемой доступа, минуя "узкие места" или разрушенную инфраструктуру связи, уже работают.



Инсталляция самодельных направленных антенн для установки радиосвязи. За счет дешевых компонентов их можно собирать даже из технологичного мусора.



Вот как это может выглядеть в итоге

К примеру, если организовать mesh-сеть из смартфонов (для этого достаточно программной модификации) и нескольких маломощных БСок (можно даже фемтосот), то "выбивая" отдельные сегменты такой системе, никакого серьезного урона ей не нанести. Да, за счет высокой частоты работы (от 900 МГц) такая сеть будет нуждаться в частых ретрансляторах, но несколько городских

кварталов захватить она вполне в силах. Кстати, сама концепция mesh-сетей следует именно из этого постулата - из того, что значительное большинство элементов сетевой инфраструктуры может "принять на себя" обслуживание абонентов в случае выхода из строя соседней базовой станции, соседнего хотспота и т.д. Если хватит мощности, конечно. Понятно, что промышленные системы в этом отношении действуют "на автопилоте" и потеря даже значительной части базовых станций им не страшна с т.з. успешной связности и предоставления сервиса (хотя, качество, конечно, упадет). Для маленьких, "карманных" сетей все придется настраивать "руками". Но их достоинство в том, что действуют они как пчелы – небольшой размер, не очень великий урон, но для их уничтожения необходимо приложить громадное количество усилий.

Если посмотреть как это реализуется на практике, то сразу вспоминаем проект Palisades в Афганистане — здесь вышки сотовой связи ставят на территории военных баз США. Частотным регулированием, понятное дело, никто не занимается, поэтому мощность можно настраивать на максимум, как и использовать наиболее выгодные для работы "нижние" диапазоны частот. Кстати, контролируя сотовую связь в военном и гражданском сегментах, радиоразведка войск США позволяет получать огромное количество информации от противоборствующих сторон (привет, мобильным модулям системы «Эшелон»!). Ведь уже мало кто передает оперативную и боевую информацию по рации — голоса не хватает для оперативного управления войсковыми и специальными операциями. А огромные потоки данных можно "прокачать" только через Wi-Fi, WiMAX или UMTS-сети с поддержкой HSPA.



Небольшие местные радиосети вполне можно объединить в «облако»

Что применяют на практике для выхода в Сеть? Это либо стационарный "пост связи", либо мобильный, смонтированный на бронированном и/или закамуфлированном автомобиле. Самый оперативный вариант - автомобиль с инсталлированной спутниковой тарелкой Ka-диапазона (80 см в диаметре), в котором установлено несколько направленных Wi-Fi антенн, которые могут "добивать" на расстояние в несколько сотен метров (частота 2,4 ГГц), или мини-БС на частоте от 450 до 2100 МГц, которая может "пробивать" сигнал и подальше. Либо вариант с радиотранслятором – он стоит на автомобиле, а БС выносится на какое-либо доминирующее здание в пределах прямой видимости: тогда можно «накрыть» площадь в несколько квадратных километров. Вопрос с автономным питанием такого комплекса волне легко решить с помощью переносных дизельгенераторов, а скрытность и мобильность достаточно высоки. Поэтому подогнать небольшой микроавтобус или джип можно практически в любую точку страны, даже охваченной беспорядками, несложно.



Носимый комплект "интернет в чемодане" – экспортный вариант, где все чисто и красиво: собрать это можно в любой лавке, где торгуют электроникой

Второй вариант — это мобильный носимый комплект: т.н. "интернет в чемодане". Его типичный состав – сетевое оборудование и направленные антенны для различных средств связи. Достаточно электропитания и можно развернуть мини-сеть и подключить абонентов к стационарному (более скоростной вариант) или беспроводному каналу связи (радиорелейка, ADSL или Ethernet, возможен и VSAT).

По сути, такой «чемоданчик» позволяет создать "изолированную сетевую инфраструктуру, которую невозможно контролировать, нельзя отследить и очень трудно уничтожить". Такой "чемодан" позволяет создать собственный интернет в условиях, когда все остальные средства связи блокированы государством. Специальное программное обеспечение позволяет включенным в сеть компьютерам и мобильным телефонам свободно обмениваться информацией и выходить во всемирную паутину без создания единой точки доступа.

В комплект каждого устройства включается также совсем недорогой нетбук для администрирования этой системы, необходимое число роутеров или модемов, а также коробка с флешками для распространения систем подключения и ПО для шифрования отправляемых сообщений (CD уже не актуальны). Туда же обычно записывают малый набор мобильного офиса — офисные приложения, которые могут работать без установки на компьютер, коммуникационное ПО, а также список адресов с прокси-серверами, фотохостингами и т.д. Не забудем и про наш любимый Tor. То есть практически все, чтобы создавать текстовые и графические сообщения, обрабатывать видео и выпускать всю эту информацию в открытую сеть Интернет. Мобильный же сегмент этой системы нужен для локального обмена информацией.



Самодельные антенны проекта FabF– бьют далеко, а стоят копейки

Есть вполне гражданские примеры работы подобных систем - к примеру, сети FabFi, которые разворачивают в Африке. Здесь в единую сеть пытаются объединить маршрутизаторы Wi-Fi, а также

нетбуки, которые могут получить питание от батарей с солнечными элементами. Связь между такими "беспроводными локалками" осуществляется с помощью достаточно простых усилителей и антенн, которые можно собрать буквально своими руками. :) Стартовый бюджет для организации сетевой инфраструктуры для нескольких городских кварталов составляет всего-то 500 долларов. Думаю, такие комплекты хорошо было бы создавать для России – проникновение фиксированного, да и мобильного интернета в нашей стране, особенно в регионах, далеко от идеала.



Загадочные мужчины на фоне самоделки – то ли сотрудники гуманитарных миссий, то ли доблестные американские разведчики. Скорее всего – обе роли сразу.

А вот для тоталитарных государств с развитой системой радиоконтроля и "глушения" подобных "постов связи" придуманы и другие решения. К примеру, мощный сигнал Bluetooth, который исходит от стационарного устройства: по сути, сотовый телефон в SSID которого обозначен призыв загружать туда свои оппозиционные видеоролики. Как только его память заполнена, у устройства меняют карту памяти, а весь "улов", после фильтрации, передается в глобальный Интернет и выставляется на фото в видеохостинги, в блоги.

Вполне возможно настроить Bluetooth таким образом, чтобы видеосъемка того или иного события будет автоматически пересылаться с одного аппарата на другой в рамках сети "доверенных пользователей". Как только эти устройства будут находиться недалеко друг от друга, конечно. Причем, от пользователей для этого не надо будет предпринимать никаких дополнительных действий.

Или "кочующие" фемтосоты, подключенные через проводные каналы доступа в Сеть к зарубежным провайдерам связи: они работают в режиме бесплатного роуминга и позволяют выходить в Интернет прямо с телефонов локальных абонентов.

Путей распространения информации, с помощью «теневого интернета», придумано много. В сочетании с использованием анонимных прокси (к примеру, того же Tor), с помощью таких беспроводных "постов связи" можно действительно выкладывать информацию в Сеть без какого-либо опознания ее отправителей. Интересно, можно ли эти системы применить и для извлечения прибыли?