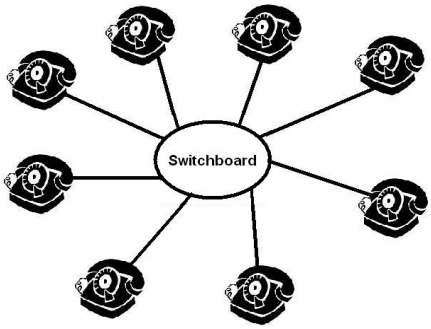
The Taking Of The Internet

The Internet was not designed for control. In fact, its fundamental design characteristic, ***de****centralization*, makes control very difficult.

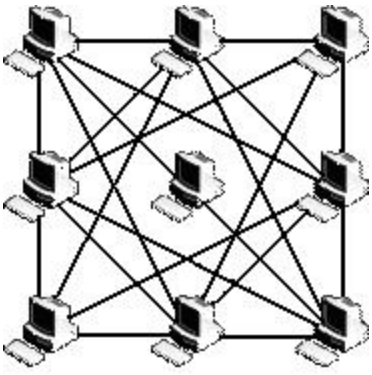
This centralized/decentralized control issue is illustrated below.

On the left is a network structure that is suited to control: A typical telephone system, where everything goes through a central switchboard. Control just one point - the switchboard - and you control everything. We call this a *star* network.

On the right is a *mesh* network. There are multiple paths between any one point on the network and any other point. This arrangement is very difficult to control.



Star Network



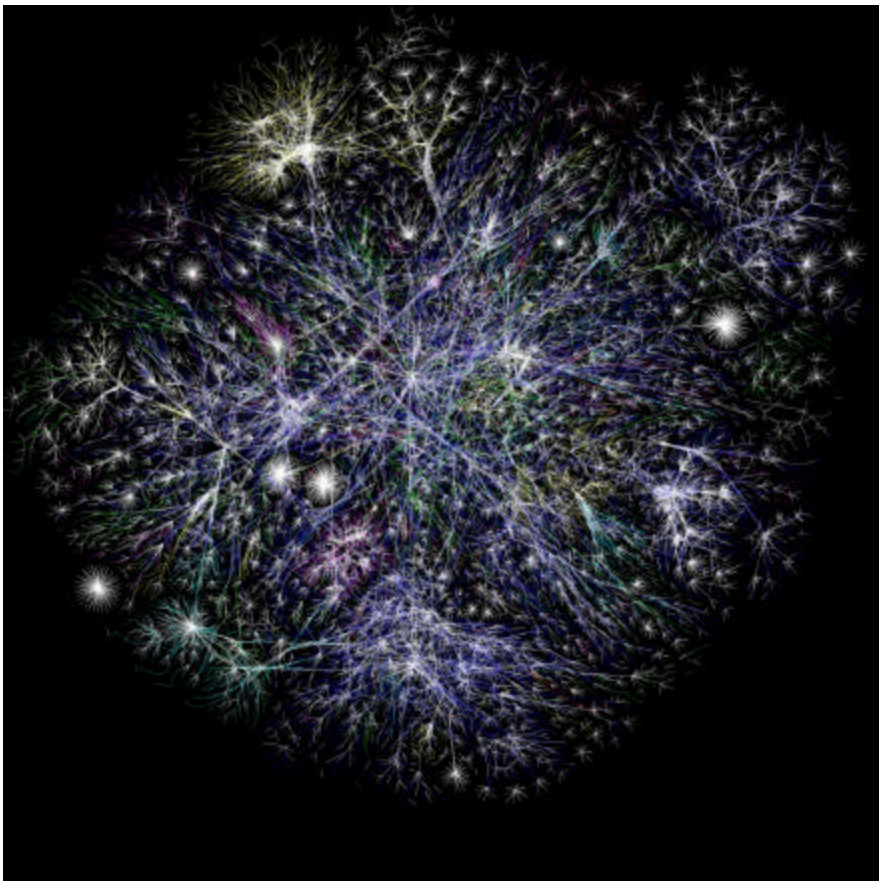
Mesh Network

The little stroke of genius that made the mesh network possible was this: Rather than putting all the intelligence in one place (like at the switchboard), distribute it everywhere, with a little bit at each autonomous machine.

When you send a message over the Internet, every packet of data you send contains the destination address, and it can find its way to the other end independently. Each routing point

sends the data forward however it can. If one link along the path is broken, the data packets just route around it, never consulting a central point for permission or instructions.

This is what the Internet looks like now:



Taming a giant mesh network like this is nearly impossible; even controlling it to any significant extent entails changing the structure of the network, and that takes time.

THE STRANGE ORIGIN OF THE INTERNET

The Internet has a very odd genesis. It was created with government funding, but it was not the type of system that any control-minded person (as most government people are) would ever authorize.

But, an odd thing happens when politicians get really scared: They grudgingly call in the smart guys and let them loose. Most of us learn about this in elementary school: The smartest kid in the class is more or less abused until the class gets into real trouble; then they run straight to him and promise to do whatever he says.

That was how the Internet was created. It was a "smartest kid" project.

The event that scared the politicians was Sputnik. The USSR surging ahead of the United States in space meant that the US had to pull out all the stops. The resulting *Advanced Research Projects Agency* (ARPA) was where the Internet was born.

The Internet – the unexpected creation of the post-Sputnik smart guys – eventually birthed a new world of information exchange. Never before have men and women been able to communicate with almost any other person in the world, regardless of distance and almost without cost. This is a completely new, deeply intimate and immensely hopeful set of abilities.

But, as in the schoolyard, once the smart kid creates something to save everyone, the others want to take it over. In this case, however, the smart kids created something that is too serious to allow anyone to control – something that reaches down to the soul – deep, voluminous, personal communications.

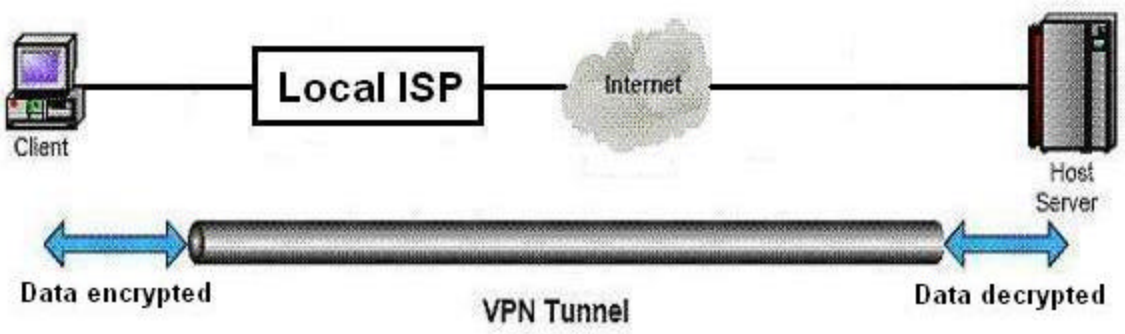
The control of criminals is good, even noble, but to control the Internet is to control massive flows of human thought. In a very real way, it is a conquest of the human soul, and no man, or group of men, has that right.

THE TAKING & THE DEFENSE

The Internet is being taken - as a conquest - by changing the structure of the Internet's mesh network. The first step is to setup choke points. This is accomplished by asserting control over all Internet Service Providers (ISPs).

Governments world-wide are passing laws that force local ISPs to monitor and record everything you do online. Then, if the police or the Feds want a record of your online activity, the ISP must provide it, and in many cases is forbidden (under pain of imprisonment) from letting you know that an inquiry was made.

Fortunately, bypassing these choke points is fairly easy. It involves creating a *VPN* (Virtual Private Network) connection from your computer to the other side of the ISP. Here's what that looks like:



This type of connection is often called a "tunnel," because it tunnels through your ISP. Your traffic still passes through the ISP, but it is encrypted, so there is no intelligible information that can be seen, just a long string of gibberish that looks something like this:

```
FK9Hs1uYFt7hOpSJUHlmYcrHjXdHrnUiFB3bM/36Ceq8OBcNDyYzGKgdieFvokId
3a9tA32uS0yrKEsxDZTItv/7ZJoj5H+D1CsU+bnnGwRy3I5vHytFDRnJOFpn2wFc
rUp7rSavV65tirOlagEIvf/AODY9yGH22HY75ChCPo9SP9P3SOvm1nEkBbDd6WK9
aMhAbZf5y1Rs6iCkRG2EHADlXupU2AIctC0SGZieYNF...
```

The other technique for asserting control over the Internet, and the harder one to evade, is mass surveillance.

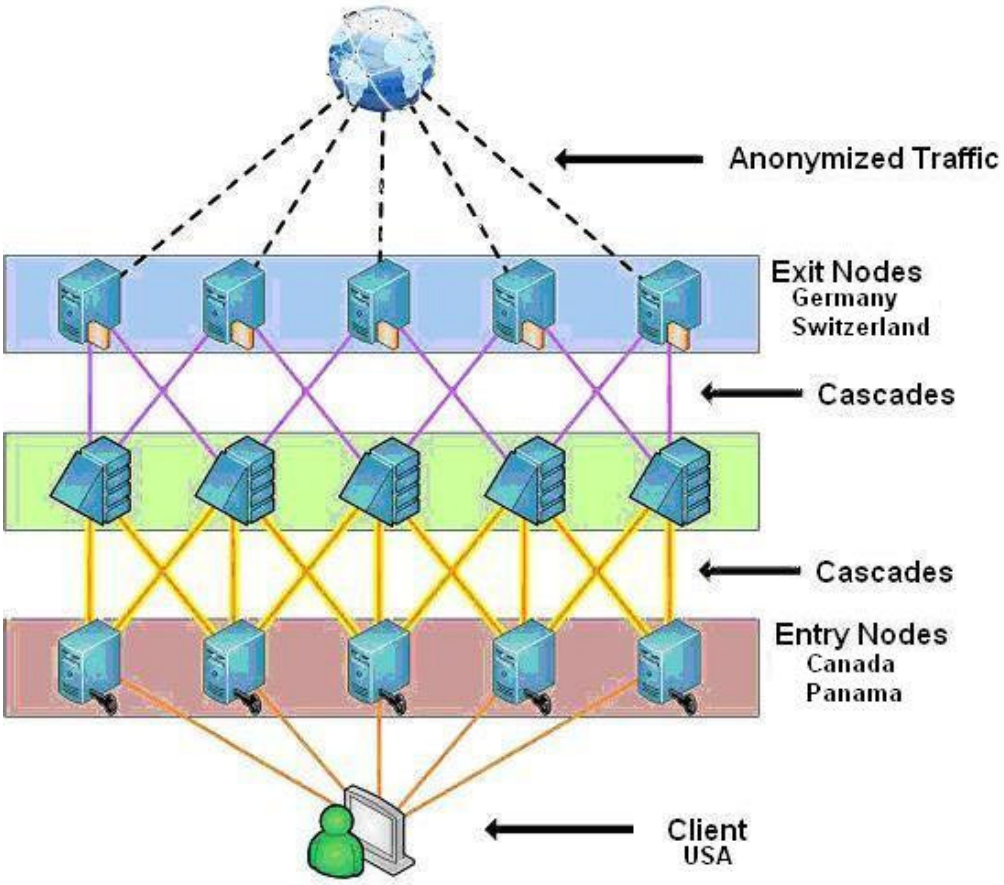
The US, the UK, most of the EU nations, China, Russia, and other states are conducting mass Internet surveillance continuously. Plenty of criminal groups and semi-autonomous intelligence agencies are doing it too. It's not as expensive as you might think, and certainly within the budget of an international player.

The VPN tunnel shown above is great for beating the choke point, but it is not effective for beating mass surveillance. By watching the amount of traffic that comes to your ISP and matching it with what comes out the other side of the tunnel, the watcher can simply pick up the trail there.

In order to beat mass surveillance, two more steps are required:

1. Obscuring the traffic much better.
2. Removing your return address.

These two things are accomplished with an anonymity network. Here is a simplified view the anonymity network we operate at Cryptohippie:



In this example, the client is in the US and a VPN tunnel runs from their computer to an entry node in either Canada or Panama, where the return address is also stripped-off. This means that a single surveillance operation is likely to lose the traffic here.

Then, the traffic goes through one or more cascades. Think of this as a MixMaster for data.

Finally, it comes out the other side in still another jurisdiction, where the network's return address is added, so the sites you visit can respond to you anonymously.

There is more to our operation than this (we do some exotic things like rotating IP addresses), but this is how mass surveillance is beaten.

A network of this type allows you to surf the web, use voice communications like Skype, email, chat, download files, etc., while remaining anonymous. At any point, it can be seen that signals are being sent, but the point of origin (and with it your identity) remains unknown.

FIGHTING THE FEAR

The conquest of the Internet – the building of what we call an Electronic Police State – has one primary foundation: Fear, which legitimizes the entire operation.

You'll notice that every time something goes wrong online, "more control" is immediately demanded as the solution. This is irrational, and here's why: We've had ever-more control for a long time, and the problems remain. The magic of control hasn't worked.

Protection from terrorists is accomplished by shooting them with bullets, not by grabbing every bit of personal information from kids, grandmas and businessmen. We all know pretty well who the terrorists are and where they live… monitoring every penny that goes in and out of Butte, Montana is not going to help them get shot.

Anti-privacy (pro-Electronic Police State) arguments pretend that central control produces perfection, which is ridiculous. We've had mass-centralization since the early 20th Century, yet we still have an overflow of terrorists and crooks. Why would we demand more of it at every possible opportunity? It's crazy.

WHAT NOW?

The Internet is being taken. Individuals who are willing to hire professional help are still able to protect themselves, but the situation continues to degrade.

We have no "action steps" to recommend, but if you care about the Internet, you should do something… while you still can.