Central Point of Control: a technology used by repressive regimes to limit internet access.

Part of my work as an independent IT engineer has been to warn new employees that their employers have the right to monitor their use of the internet and even read their e-mails (and to fire them for their transgressions, minor or otherwise). This makes me feel less guilty when I install the surveillance technology for the company intranet. Imagine that your country is like a large company, with one intranet and one e-mail system. You have no choice but to comply with the rules. Resistance is futile.

Cuba and Burma are two “good” examples of state control of the internet. Control is by restricting access through censorship, filtering and surveillance. In fact, you can’t go beyond the country intranet except by special permission and in state-run locations. The state has the right to monitor your internet use and your e-mails, and to “fire” you if necessary for reasons of state security. There is only one internet service provider: the state. This is different from the case of China, where internet access is not normally restricted except through self censorship: you are told to behave or else... Some emerging dictatorships (Venezuela is an example) are in the process of deciding which of these internet control “models” it will adopt.

Iran is probably something in between. All commercial Internet Service Providers (ISPs) are required to connect via the government controlled Telecommunication Company of Iran (TCI). The state-managed central point of control facilitates the implementation of internet filtering and the surveillance of internet use as all traffic from the ISPs serving households is routed through TCI. It is worth keeping in mind that Iran ranks only slightly higher than North Korea on freedom of expression.

There was recently a debate in Venezuela on whether to introduce a central point of control, Iranian style, but the idea seems to have been dropped from the proposed *media censorship law* now going through the regime-controlled legislature. The Cuban model is not applicable because internet access is already too widespread in Venezuela, where around 35% of the population has full access to internet (compared to a nominal 14% with very limited access in Cuba). Establishing a central point of control in

Venezuela would require a large investment in expertise, money and technology. Cuba can’t help their Venezuelan allies much because they fall short in all these resources.

#SOSinternetVE

There has been considerable rejection in Venezuela of the idea of a central point of control. On Thursday 16th of December 2010, the Twitter tag most visited worldwide was #SOSInternetVE. The tag was created to express disagreement with the internet censorship law in the process of approval by the Venezuelan legislature. This type of initiative can put considerable pressure on repressive regimes such as Venezuela's, and can help to curb the worst excesses against freedom of expression elsewhere in the world.

Some Latin-American countries (Brasil, Chile, Argentina, Colombia and Perú) have implemented central points of control, or Network Access Points (NAP), with no sinister censorship intentions. These are known locally as *punto único de acceso*. Here are some Wikipedia links:

The term NAP is now rarely used. The term in current use is "internet exchange point” (IX or IXP). There are around 300 IXPs around the world, none in Venezuela. IXP refers to a physical infrastructure through which internet service providers (ISPs) exchange Internet traffic between their networks (autonomous systems). IXPs reduce the portion of an ISP's traffic which must be delivered via their upstream transit providers, thereby reducing the average per-bit delivery cost of their service. Furthermore, the increased number of paths learned through the IXP improves routing efficiency and fault tolerance.