THE UNNAMED NETWORK PROVIDER EXPOSING OUR INFRASTRUCTURE

Today was Global Threat day, when James Clapper testifies before various committees in Congress and Ron Wyden asks uncomfortable questions (today, directed exclusively at John Brennan). I'll have a few posts about the hearings (in Senate Armed Services and Senate Intelligence Committees) and Clapper's testimony, the SASC version of which is here.

One interesting detail in Clapper's testimony comes in the several paragraph section on Infrastructure within a larger section on "Protecting Information Resources." Here's how the testimony describes the Juniper hack.

> A major US network equipment manufacturer acknowledged last December that someone repeatedly gained access to its network to change source code in order to make its products' default encryption breakable. The intruders also introduced a default password to enable undetected access to some target networks worldwide.

There's no discussion of how many Federal agencies use Juniper's VPN, nor of how this must have exposed US businesses (unless the NSA clued them into the problem). And definitely no discussion of the assumption that NSA initially asked for the back door that someone else subsequently exploited.

More importantly, there's no discussion of the cost of this hack, which I find interesting given that it may be an own goal.