RETALIATING AGAINST STATE-SPONSORED CYBER WAR

On the first news day after the holiday weekend reporting on Lockheed Martin, WSJ reports that the US is moving towards making cyberattacks an act of war.

> The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force.

And they're building into this policy an assumption that the biggest attacks must have state sponsorship.

> Pentagon officials believe the most-sophisticated computer attacks require the resources of a government. For instance, the weapons used in a major technological assault, such as taking down a power grid, would likely have been developed with state support, Pentagon officials say.

This new policy won't be subject to intelligence manipulation at all, nosiree!

The next time someone wants to invent a casus belli against Iran, they can just point to a particularly successful hack and (ignoring all questions about appropriate retaliation for Stuxnet…) claim the Iranians have done it and say it, like evidence of WMD, is classified.

They already presumably fabricated one Laptop of Death for Iran, why not another?

And then, declaring ourselves incompetent to retaliate via cyberspace (Stuxnet notwithstanding), they'll have their excuse to

roll out the war machine.