BREAKING: PANETTA EQUATING CRUDE IRANIAN CYBERATTACKS WITH PEARL HARBOR, IRAN INFILTRATED ARAMCO

Today, the NYT—serving its role as spokesperson for the Cold War against Iran—confirms what blabby Joe Lieberman told CSPAN last month: the government suspects Iran was behind a series of crude cyberattacks on US banks.

Or to put it differently, Leon Panetta wants us to be more afraid of crude DNS attacks on US online banking sites than he wants us to be of the orders of magnitude greater damage the banks cause all by themselves. Because … Iran!

More interesting is the widely reported speculation we think Iran was behind the more serious attack on Aramco.

> The attack under closest scrutiny hit Saudi Aramco, the world's largest oil company, in August. Saudi Arabia is Iran's main rival in the region and is among the Arab states that have argued privately for the toughest actions against Iran. Aramco, the Saudi state oil company, has been bolstering supplies to customers who can no longer obtain oil from Iran because of Western sanctions.
>
> The virus that hit Aramco is called Shamoon and spread through computers linked over a network to erase files on about 30,000 computers by overwriting them. Mr. Panetta, while not directly attributing the strike to Iran in his speech, called it "probably the most destructive attack that the private

> sector has seen to date."
>
> Until the attack on Aramco, most of the cybersabotage coming out of Iran appeared to be what the industry calls "denial of service" attacks, relatively crude efforts to send a nearly endless stream of computer-generated requests aimed at overwhelming networks. But as one consultant to the United States government on the attacks put it several days ago: "What the Iranians want to do now is make it clear they can disrupt our economy, just as we are disrupting theirs. And they are quite serious about it."

That's interesting not because the attack did real damage—it didn't, because it hit the business, not the production, computers.

> Saudi Aramco has said that only office PCs running Microsoft Windows were damaged. Its oil exploration, production, export, sales and database systems all remained intact as they ran on isolated and heavily protected systems.
>
> "All our core operations continued smoothly," CEO Khalid Al-Falih told Saudi government and business officials at a security workshop on Wednesday.
>
> "Not a single drop of oil was lost. No critical service or business transaction was directly impacted by the virus."

It's interesting because the malware was introduced into the Aramco network by an insider.

> One or more insiders with high-level access are suspected of assisting the hackers who damaged some 30,000 computers at Saudi Arabia's national oil company last month, sources familiar

> with the company's investigation say.
>
> [snip]
>
> The hackers' apparent access to a mole, willing to take personal risk to help, is an extraordinary development in a country where open dissent is banned.
>
> "It was someone who had inside knowledge and inside privileges within the company," said a source familiar with the ongoing forensic examination.

Once you translate the NYT's spin, here's what we're left with:

- We're supposed to treat cyberattacks by Iran as an existential threat, even though they expose Iran's relative impotence in the cyber sphere.
- We're supposed to get panicked about computers here at home because Iran succeeded in human espionage with Aramco.

And while Panetta cries wolf over and over, the banksters and the oil companies continue to real damage he ignores.