PANETTA MISSES UNDERLYING PROBLEM WITH CYBERWHINES

We can play a game we often play here at emptywheel with Leon Panetta's address on cybersecurity last night. For each major attack he discusses or potential threat he envisions, there is an equivalent one that has or could easily happen without the cyber component.

Panetta talks about the Shamoon malware that hit Aramco infecting 30,000 computers.

> But even more alarming is an attack that happened two months ago when a very sophisticated virus called Shamoon infected computers in the Saudi Arabian State Oil Company Aramco. Shamoon included a routine called a 'wiper', coded to self-execute. This routine replaced crucial systems files with an image of a burning U.S. flag. But it also put additional garbage data that overwrote all the real data on the machine. More than 30,000 computers that it infected were rendered useless and had to be replaced. It virtually destroyed 30,000 computers.

But how did that do more damage than the Richmond Refinery fire and subsequent spike in gas prices, likely caused by a corroded pipe neglected in a recent turnaround? How did that do more damage than the damage BP, Transocean, and Halliburton did when their negligence led to the Deepwater Horizon spill, which still appears to be leaking 31 months later?

Panetta talks about DDS attacks on banks that disrupted customer websites.

> In recent weeks, as many of you know, some large U.S. financial institutions were hit by so-called Distributed Denial

> of Service attacks. These attacks delayed or disrupted services on customer websites. While this kind of tactic isn't new, the scale and speed with which it happened was unprecedented.

How is this worse than the damage done by repeated flash crashes and other irregularities caused by high frequency trading? To say nothing of the damage done by reckless gambling during the housing crisis, which wiped out trillions of dollars in wealth?

Panetta talks about passenger or transport trains derailing.

> They could, for example, derail passenger trains or even more dangerous, derail trains loaded with lethal chemicals.

Apparently Panetta is unaware that trains derail all the time, and even spill dangerous chemicals, often because of operational or maintenance issues.

To some degree we could continue this game indefinitely, always finding an equivalent threat to the imagined or real threat posed by a cyberattack.

But there is a logic to the game: it reveals not only that Panetta is fearmongering while ignoring the reality of equally or more dangerous non-cyber threats.

It suggests that he—and frankly, the rest of government trying to address this problem—misunderstands why corporations are not responding to the serial fearmongering about cyber. If corporations refuse to take obvious precautions against cyberthreats, but also refuse to take obvious precautions against non-cyberthreats, it suggests the problem is not the cyber component in the least.

The problem is that these corporations don't

want to—and in many cases refuse to—take obvious precautions against risk in general.

This suggests, then, that these corporations have not been given the sufficient combination of carrot and stick generally to mitigate obvious risks. And giving them immunity for cyber-negligence is likely not going to mitigate the threat reckless, negligent corporations pose to our society, whether because our enemies cause them to do things, or whether they do them of their own accord.

The problem is a culture that encourages corporations to skirt all accountability. No amount of fancy programmers are going to change that by themselves.