HACKERS PENETRATE FREEDOM; THE SHIP HAS ALREADY SAILED

Reuters has a report I found sort of punny, about how white hat hackers had managed to break into the computer systems of the lead ship of the Navy's Littoral Combat Ship program, the USS Freedom.

> A Navy team of computer hacking experts found some deficiencies when assigned to try to penetrate the network of the USS Freedom, the lead vessel in the $37 billion Littoral Combat Ship program, said the official, who spoke on condition of anonymity.
>
> The Freedom arrived in Singapore last week for an eight-month stay, which its builder, Lockheed Martin Corp., hopes will stimulate Asian demand for the fast, agile and stealthy ships.

It may be ironic that Lockheed had a ship get hacked just before it sent the ship out on a sales trip to Asia. (Asia! Where our most fear hacking-rival is!)

But … um, Lockheed?

Lockheed, of course, couldn't keep the F-35 program safe from hackers either, and that time it wasn't white hats doing the hacking.

Before the government imposes fines for companies unwilling to sacrifice the security of their systems to program in a backdoor, as the WaPo reports is being debated …

> A government task force is preparing legislation that would pressure companies such as Facebook and Google to enable law enforcement officials to intercept online communications as they occur, according to current and former

> U.S. officials familiar with the effort.
>
> [snip]
>
> Susan Landau, a former Sun Microsystems distinguished engineer, has argued that wiring in an intercept capability will increase the likelihood that a company's servers will be hacked. "What you've done is created a way for someone to silently go in and activate a wiretap," she said. Traditional phone communications were susceptible to illicit surveillance as a result of the 1994 law, she said, but the problem "becomes much worse when you move to an Internet or computer-based network."
>
> Marcus Thomas, former assistant director of the FBI's Operational Technology Division, said good software coders can create an intercept capability that is secure. "But to do so costs money," he said, noting the extra time and expertise needed to develop, test and operate such a service.

… Maybe we ought to instead focus on Lockheed's apparent inability to keep the hundreds of billion dollar weapons systems it produces safe from hackers?