TIME TO OUT THE CYBER-INSECURE DEFENSE CONTRACTORS

In its latest update on Chinese hacking of our defense programs, WaPo provides a list of defense programs that have been compromised, which includes many of our most important and error-prone programs.

> The designs included those for the advanced Patriot missile system, known as PAC-3; an Army system for shooting down ballistic missiles, known as the Terminal High Altitude Area Defense, or THAAD; and the Navy's Aegis ballistic-missile defense system.
>
> Also identified in the report are vital combat aircraft and ships, including the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the Navy's new Littoral Combat Ship, which is designed to patrol waters close to shore.
>
> Also on the list is the most expensive weapons system ever built — the F-35 Joint Strike Fighter, which is on track to cost about $1.4 trillion. The 2007 hack of that project was reported previously.

WaPo also, having seen classified sections of a report that had previously been released in unclassified form, also places more emphasis on the potential impact not just of cybertheft, but cyber-sabotage, than it has in the past, basically pointing to this section of the report itself.

> The threats described in the previous section [which focus on sabotage at the microchip level] may impose severe consequences for U.S. forces engaged in

> combat:
>
> - *Degradation or severing of communication links critical to the operation of U.S. forces, thereby denying the receipt of command directions and sensor data*
> - *Data manipulation or corruption may cause misdirected U.S. operations and lead to lack of trust of all information Weapons and weapon systems may fail to operate as intended, to include operating in ways harmful to U.S. forces*
> - *Potential destruction of U.S. systems (e.g. crashing a plane, satellite, unmanned aerial vehicles, etc.).*
>
> At the national level, one could posit a large-scale attack on the U.S. critical infrastructure (e.g., power, water, or financial systems). An attack of sufficient size could impose gradual wide-scale loss of life and control of the country and produce existential consequences.

WaPo also provides a hint at our solutions and Chinese counter-responses. That is, as our prime contractors have become more adept at cyber-security, China has moved onto attack

subcontractors.

> In an attempt to combat the problem, the Pentagon launched a pilot program two years ago to help the defense industry shore up its computer defenses, allowing the companies to use classified threat data from the National Security Agency to screen their networks for malware. The Chinese began to focus on subcontractors, and now the government is in the process of expanding the sharing of threat data to more defense contractors and other industries.

Yet the government won't take the obvious step of tying ongoing contracts to cyber-security, instead requiring only that contractors provide the government notice of cyber-attacks.

> An effort to change defense contracting rules to require companies to secure their networks or risk losing Pentagon business stalled last year. But the 2013 Defense Authorization Act has a provision that requires defense contractors holding classified clearances to report intrusions into their networks and allow access to government investigators to analyze the breach.

What's most interesting about all this, though, is that the report (at least the classified list the WaPo saw) didn't identify via which contractors in the supply chain China hacked these programs. But the US is not, apparently, keeping all of that information secret from China.

> U.S. officials said several examples were raised privately with senior Chinese government representatives in a four-hour meeting a year ago. The officials, who spoke on the condition of anonymity to describe a closed meeting,

> said senior U.S. defense and diplomatic officials presented the Chinese with case studies detailing the evidence of major intrusions into U.S. companies, including defense contractors.
>
> [snip]
>
> The list did not describe the extent or timing of the penetrations. Nor did it say whether the theft occurred through the computer networks of the U.S. government, defense contractors or subcontractors.

So if the government is sharing at least some details of what it knows about China's hacks with China, then why is it keeping details about which contractors taxpayers are paying lots of money for cyber-attack induced rework to? Why can't it provide at least skeletal information about which contractors have let China compromise our security so much?