WIKILEAKS REVEALS THAT CHINA ALREADY KNOWS WHAT WIKILEAKS REVEALS

I've been bitching and bitching and bitching and bitching about DOD's refusal to fix the gaping holes in its network security even while it cries that Bradley Manning allegedly downloaded a bunch of cables using those gaping holes. As I point out, if all it took Manning to get all these databases was one Lady Gaga CD, then presumably our enemies can and do get what they want pretty easily, too.

As citizens, we just don't ever find out about those other data breaches.

Well, apparently someone leaked a set of previously unreported WikiLeaks cables to Reuters, which used them as one of many sources to report on how much data China is just hacking from our government networks, including the sieve-like DOD ones.

> Secret U.S. State Department cables, obtained by WikiLeaks and made available to Reuters by a third party, trace systems breaches – colorfully code-named "Byzantine Hades" by U.S. investigators – to the Chinese military. An April 2009 cable even pinpoints the attacks to a specific unit of China's People's Liberation Army.
>
> Privately, U.S. officials have long suspected that the Chinese government and in particular the military was behind the cyber-attacks. What was never disclosed publicly, until now, was evidence.
>
> U.S. efforts to halt Byzantine Hades hacks are ongoing, according to four sources familiar with investigations. In

> the April 2009 cable, officials in the State Department's Cyber Threat Analysis Division noted that several Chinese-registered Web sites were "involved in Byzantine Hades intrusion activity in 2006."
>
> [snip]
>
> What is known is the extent to which Chinese hackers use "spear-phishing" as their preferred tactic to get inside otherwise forbidden networks. Compromised email accounts are the easiest way to launch spear-phish because the hackers can send the messages to entire contact lists.
>
> The tactic is so prevalent, and so successful, that "we have given up on the idea we can keep our networks pristine," says Stewart Baker, a former senior cyber-security official at the U.S. Department of Homeland Security and National Security Agency. It's safer, government and private experts say, to assume the worst — that any network is vulnerable. [my emphasis]

Oh, okay.

Our government has apparently conceded it can't keep its networks secret from China.

I'm not surprised, mind you. While I assume the problems at DOD are a worst case scenario (because of its size and logistical issues stemming from all the wars we're running), the size of the gaping holes at DOD (and the lackadaisical attitude DOD has about closing them) shows how low a priority network security is in our government generally.

Plus, Chinese hackers are that good.

But the confirmation that China can basically just take what it wants at will really raises new questions about our government's treatment of Bradley Manning specifically and its hyper-

secrecy more generally.

If we're not keeping all these secrets from China, our biggest rival, who are we keeping them from? If our adversaries can just go and get whatever they want off our networks, then why has the government treated Bradley Manning's allegedly doing the same a capital offense? And if our government has just conceded that China can take what it wants, then why won't it let its own citizens know what China presumably already knows?