

THE BULLSHIT EXCUSES FOR NOT RETALIATING FOR OPM

A handful of anonymous sources have given Ellen Nakashima some bullshit explanations for why the Administration is not retaliating against China for the OPM hack.

Most laughable is that they're willing to retaliate for "economic" spying but not "political" spying. While also mentioning the Sony example, Nakashima points to the DOJ case against Chinese hackers for eavesdropping on discussions about trade disputes from the steel industry.

As a result, China has so far escaped any major consequence for what U.S. officials have described as one of the most damaging cyber thefts in U.S. government history – an outcome that also appears to reflect an emerging divide in how the United States responds to commercial vs. traditional espionage.

Over the past year and a half, the United States has moved aggressively against foreign governments accused of stealing the corporate secrets of major U.S. firms. Most notably, the Justice Department last year filed criminal charges against five Chinese military officers accused of involvement in alleged hacks of U.S. Steel, Westinghouse and other companies.

Nakashima doesn't say whether her sources made this connection or she did, but it's an inapt example. As I pointed out at the time, spying on trade negotiation adversaries is precisely the kind of "commercial" spying we embrace. We do this *all the time*. DOJ chose to indict on those trade dispute discussions but not on a never-ending list of hacks against more sensitive

targets – like the F-35 development team – that fit more comfortably (though still not entirely) in the kind of “economic” spying we fancy others do but we don’t; DOJ probably made that choice because both the target and the evidence was segregable from more sensitive issues (the Chinese government and our clusterfuck of DOD contracting cyberdefense). In other words, it is not (as Nakashima claims uncritically) an example of the split between political and economic spying we claim to adhere to. That indictment is far better understood as us indicting Chinese hackers for something we not only do but also falls into what is considered acceptable spying internationally – that is, us trying to subject the rest of the world to our legal system – but doing so in an area where we won’t have to give any secrets away to prosecute.

The rest of the WaPo story focuses on another nonsensical explanation for not going after China: to avoid revealing sources and methods.

“We have chosen not to make any official assertions about attribution at this point,” said a senior administration official, despite the widely held conviction that Beijing was responsible. The official cited factors including concern that making a public case against China could require exposing details of the United States’ own espionage and cyber capabilities.

Again, this is nonsensical and should not have been repeated uncritically.

The FBI and everyone else has been happy to blame North Korea for the Sony hack. But we’ve gotten no more proof there than we have that China is behind the OPM hack. Rather than exposing sources and methods to prove attribution, the government simply said, “trust us.” There’s no reason they couldn’t do the same here (indeed, that’s what they have been saying in secret). The Sony hack is proof that the

government doesn't feel like it needs to offer proof before it blames another country for a hack.

There are two far more likely reasons we're not retaliating against China in this case (though the fact that we do this kind of stuff to China all the time – and they could happily point to proof of that to demonize us in response – is one of them).

First, we simply don't "retaliate" against countries that are big enough to fight back (as Nakashima's other example, of the Russian hack of State for which we haven't retaliated, makes clear). It's one thing to go after a group of hackers from which China can claim some plausible deniability. It's another to go after China itself.

Finally, Nakashima alludes to what is probably the real reason we're going to remain quiet about this hack.

The government also is pursuing an array of counter-intelligence measures aimed at guarding against the Chinese government's ability to use the stolen data to identify federal workers who might be induced to spy for Beijing.

China has much of our intelligence community – and many other easily embarrassed types, including politicians – by the nuts right now. It knows who our spooks are, where they are, what they might know, what their fingerprints are, and what extramarital affairs they've admitted to. When someone has you by the nuts like that, it's usually a good idea to extract your nuts before you start trying to throw punches. It's going to take a long time for the US to do that.

Which strongly suggests that the more laughable excuses for not retaliating – the claim we're not blaming China because of sources and methods and some split between economic and political spying that we don't really follow – serve no

other purpose than to avoid admitting how much
China does have us by the nuts.