

CYBER-UNICORN JOURNALISTS SHOCKED THE UNICORN DIDN'T APPEAR, AGAIN

When last we checked in on claims the US was going to cyber-deter China, I suggested people should understand the underlying dynamics at work.

Before people start investing belief in unicorn cyber deterrence, they'd do well to understand why it presents us such a tough problem.

That was 11 days ago. Since then, James Clapper has claimed (I'm not necessarily endorsing this claim as true, especially given the timing) the US isn't even 100% sure China is behind the OPM hack – in part because we've lost some monitoring capabilities in recent years – all while making it clear we don't consider it an attack because we do precisely the same thing to China. At the same time, top level US and Chinese officials met in anticipation of Xi Jinping's visit. Here's the White House readout of that meeting.

From September 9-12, senior Administration officials held a series of meetings with Secretary of the Central Political and Legal Affairs Commission of the Communist Party of China Meng Jianzhu in Washington, D.C. Mr. Meng traveled to Washington as President Xi Jinping's Special Envoy to discuss cybersecurity and other issues in advance of President Xi's State Visit. Secretary of Homeland Security Jeh Johnson hosted Mr. Meng during his visit. In this capacity, Secretary Johnson convened a meeting between members of the Chinese delegation and

representatives from the Departments of State, Treasury, Justice, Federal Bureau of Investigation, and the Intelligence Community. In addition, FBI Director Comey also met with Mr. Meng at FBI headquarters for discussions. National Security Advisor Susan E. Rice received Mr. Meng for a meeting at the White House, where she had a frank and open exchange about cyber issues.

Remember: China is believed to have all of Jim Comey and Jeh Johnson's security clearance files (probably Susan Rice's as well). Comey in particular keeps raising that point. That surely adds something to such negotiations, knowing that your interlocutor has read a ready-made intelligence portfolio that your own government compiled on you.

Now the journalists who keep reporting that the US is about to, honest to god, this time they mean it, sanction China for its hacking report that sanctions are off the table for now, in part because those negotiations resulted in some kind of cyber agreement.

The United States will not impose economic sanctions on Chinese businesses and individuals before the visit of China President Xi Jinping next week, a senior administration official said Monday.

The decision followed an all-night meeting on Friday in which senior U.S. and Chinese officials reached "substantial agreement" on several cybersecurity issues, said the administration official, who spoke on the condition of anonymity because of the topic's sensitivity.

The potential for sanctions in response to Chinese economic cyberespionage is not off the table and China's behavior in cyberspace is still an issue, the

official said. "But there is an agreement, and there are not going to be any sanctions" before Xi arrives on Sept. 24, the official said.

The breakthrough averted what would have raised a new point of tension with the Chinese that could have overshadowed the meeting – and Xi's first state visit.

"They came up with enough of a framework that the visit will proceed and this issue should not disrupt the visit," the official said. "That was clearly [the Chinese] goal."

The reporting on this appears to be problematic, in part, because sources for these stories themselves misunderstand the issue.

Yet what that agreement is remains unclear. Two U.S. officials told The Daily Beast that substantial disagreement remains between the U.S. and China. China insists that it's the victim of cyber spying, not a perpetrator. But the U.S. has filed criminal charges against Chinese officials for their role in stealing trade secrets and intellectual property from American companies.

[snip]

[CSIS Deputy Director Scott] Kennedy noted that given the length of time Meng was in Washington, his visit almost certainly covered other issues, including China's efforts to hunt down Chinese nationals accused of crimes who are living abroad. U.S. law enforcement officials have complained that Chinese state security operatives are working in this country illegally and trying to intimidate Chinese people living here legally.

Remember, "US official" is journalistic code often used for members of Congress or contractors. And if these (possible) members of Congress don't understand that the US sensors embedded in China's networks are incredibly invasive cyber spying, if whoever claimed that our indictment for stealing information on trade disputes (something we spy on too) believes that we indicted for stealing IP, if those sources can't imagine we might respond to the OPM hack by cracking down on extraordinary Chinese agents in the US, then those sources aren't appreciating the real power dynamics at stake. And we're going to continue to have journalism on this topic that serves more to provide a convenient narrative than to inform.

Thank you for playing, thank you for providing the appearance of a threat to placate Congress and drive a narrative of a tough negotiation, all while not laying out how the OPM hack changes things.

Several things seem to have been missed in this recent round of cyber-deterrence unicorn reporting. While China's crashing stock market (renewed again today) provides a bit more leverage for the US against China – among other things, it raises the value Chinese elites would place on their US property and holdings, though China itself wants to pressure some of the same elites – it is still not in our best interest to antagonize this relationship. Moreover, whatever additional leverage we've got economically is more than offset by the OPM and related hacks, which China could use in any number of ways to really damage the US, especially given so many of our other critical systems – public and private, and I suspect that's part of what some of the related hacks have been designed to demonstrate – remain insecure.

Most importantly, even before the Snowden leaks, the US had a real interest in finding some kind of norms that would make the cyber realm less volatile. That's probably even more true now, because (as Clapper said, and this part I

believe) our adversaries have been hardening their own defenses while stealing information that turns out to be more valuable to the US, meaning we don't have such asymmetric advantage in the cyber realm anymore.

This comes at a time when Congress has become adamantly opposed to anything that resembles negotiations, because to them it looks like weakness. And most seem not to understand the stakes behind the reasons why the OPM hack cannot be considered an attack.

So if some credulous reporting created the space for such an agreement, great!