CLOUDSTRIKE'S OWN ANNOUNCEMENT MAKES IT CLEAR IT DOESN'T HAVE PROOF OF ONGOING CHINESE ECONOMIC CYBERATTACKS

Many many many outlets are reporting that China has continued conducting economic espionage even after Xi Jinping agreed to stop doing it. They base that claim on this post from CloudStrike, a big cybersecurity contractor that spends a lot of time feeding the press scary stories about hacking.

Here's the proof they offer:

> Over the last three weeks, CrowdStrike Falcon platform has detected and prevented a number of intrusions into our customers' systems from actors we have affiliated with the Chinese government. Seven of the companies are firms in the Technology or Pharmaceuticals sectors, where the primary benefit of the intrusions seems clearly aligned to facilitate theft of intellectual property and trade secrets, rather than to conduct traditional national-security related intelligence collection which the Cyber agreement does not prohibit.
>
> [snip]
>
> In addition to preventing these intrusions, the CrowdStrike Falcon platform also provided full visibility into every tool, command and technique used by the adversary. This allowed us to determine that the hackers saw no

> need to change their usual tradecraft or previously used infrastructure in an attempt to throw off their scent.

The include a timeline showing 9 attempted intrusions into Tech Sector companies, and 2 into Pharma companies since Xi and President Obama signed the hacking agreement.

Now, even assuming that CrowdStrike has accurately labeled these Chinese government hackers (CrowdStrike's CTO was less confident in an interview with Motherboard) this still is not proof that China has violated the agreement.

After all, the key part of the agreement is on how stolen information gets used — whether it gets used to benefit individual companies or even entire sectors (the latter of which we do in our own spying, but never mind). If CrowdStrike prevented any data from being stolen, then it is impossible to assert that it was being stolen to benefit market actors without more evidence that the hackers were tasked by a market actor. Even the indictment everyone points to as proof that China engages in economic espionage did not allege that the People Liberation's Army had shared the data involved in the single economic espionage charge with private sector companies, and given that the data in question pertained to nuclear technology ,it's not something that is proven just because it was stolen in the context of an ongoing relationship with the victim (even if that is a logical presumption to make).

The same is true here. When China hacked Google to spy on dissidents, that was clearly national security spying. When the US hacked Huawei to figure out how to backdoor its equipment, that was clearly national security spying.When the US used Microsoft and Siemens products to carry out StuxNet, the tech companies were merely enabling targets. There are too many reasons to hack tech sector companies for solidly national security purposes to claim, just based on the sector itself, that it was done for economic espionage.

You can't even point to the 2 Pharma intrusions to make the claim. A list of sites the State Department identified as critical infrastructure from a leaked 2009 cable includes over 25 pharmaceutical sites (including animal Pharma), many of them related to vaccines. If we're treating pharmaceutical supply and research facilities as critical infrastructure, with the presumed consequent defensive surveillance of those sites, it is tough to argue the Chinese can't consider our pharmaceutical companies making key drugs to be critical targets. Both can be argued to stem from the same public health concerns.

I'm not saying it's impossible or even unlikely that these intrusions were attempted economic espionage. I'm saying that this isn't evidence of it, and that the reporting repeating this claim has been far too credulous.

But that also points to one of the inherent problems with this deal (one pointed to by many people at the time). When last he testified on the subject, Jim Clapper didn't even claim to have fully attributed the OPM hack. The same attribution and use problems exist here. China may steal data on an important new drug, but that's not going to be enough to prove they stole it *for commercial gain* until they release their own copycat of the drug in several years and use it to undercut the US company's product, and even then that may require a lot more data — collected by spying! — from inside the market companies themselves (in part because China engages in many other means of stealing data which aren't the subject of a special agreement, which will make even the copycat instance hard to prove came from an intrusion).

China knew that, too, when it signed the agreement. It will take more than evidence of 11 attempted intrusions to prove that China is violating the agreement.