DID THE OPM HACK FIX JACK GOLDSMITH'S ANONYMITY PROBLEM?

In a piece claiming "the most pressing problem the United States sees in its cyber relations with China [is] the widespread espionage and theft by China in U.S. public and private digital networks," Jack Goldsmith argues any cyber agreement with China won't be all that useful because we would never be able to verify it.

> I still adhere what I once wrote in response to this: "in the absence of decent verification, we cannot be confident that transparency measures are in fact transparent, or that revealed doctrine is actual doctrine. Nor can norms get much purchase in a world without serious attribution and verification; anonymity is a norm destroyer."

Goldsmith says this in a piece that claims to adopt Sanger's expressed concerns about the proposed deal and what it won't cover. Here's Sanger:

> But it seems unlikely that any deal coming out of the talks would directly address the most urgent problems with cyberattacks of Chinese origin, according to officials who spoke on the condition of anonymity to describe continuing negotiations.
>
> Most of those attacks have focused on espionage and theft of intellectual property. The rules under discussion would have done nothing to stop the theft of 22 million personal security files from the Office of Personnel Management, which the director of national intelligence, James R. Clapper

> Jr., recently told Congress did not constitute an "attack" because it was intelligence collection — something the United States does, too.
>
> The agreement being negotiated would also not appear to cover the use of tools to steal intellectual property, as the Chinese military does often to bolster state-owned industries, according to an indictment of five officers of the People's Liberation Army last year. And it is not clear that the rules would prohibit the kind of attack carried out last year against Sony Pictures Entertainment, for which the United States blamed North Korea. That attack melted down about 70 percent of Sony's computer systems.

So Sanger quotes James Clapper saying he doesn't consider OPM an attack (for good reason), but says that's one of the most urgent concerns about Chinese hacking. Clapper's response doesn't seem to substantiate Sanger's claim about the centrality of that as a concern, though I think it is a huge concern. I'll come back to this.

Then Sanger — in a piece that once again repeats the shitty reporting that last year's indictment showed the theft of IP to bolster state-owned industries (see this post, but I'm working on a follow-up) — says the agreement won't cover IP theft. Finally, Sanger says that the agreement might not cover a Sony pictures hack, which the Chinese haven't been accused of doing, so why would that be important in an agreement with the Chinese?

That last bit is where Goldsmith actually *doesn't* adopt what Sanger has laid out. Indeed, he seems to say the agreement *is* about Sony type hacks.

> [T]he ostensible "agreement" won't have anything to do with the most pressing

> problem the United States sees in its cyber relations with China — the widespread espionage and theft by China in U.S. public and private digital networks. The negotiation is mainly about cyberattacks (cyber operations that disrupt, destroy, degrade, or manipulate information on adversary networks) and not about cyberexpoitation (cyber operations involving theft, intelligence-gathering, and the like on digital networks).

The Sony hack certainly disrupted and destroyed the film studio's networks, even while exposing a bunch of embarrassing intelligence. But thus far, we're proceeding as if China hasn't done that to "us" (to the extent a Japanese owned film studio counts as the US), North Korea has. We don't even ever talk about whether China, in addition to robbing the F-35 program blind, also sabotaged it; I remain agnostic about whether the US defense industry needed China's help to sabotage the program, but China definitely had the persistence in networks to sabotage key parts that have since proven faulty. Plus, we're taking it on faith that claims that the NYSE/United outages that happened on the same day are really unrelated, and curiously we're not talking about the serial air travel outages we've experienced of late (after United, the FAA and then American went down because of "software problems"). I would suggest that the IC may have reason to have urgent concern about China's ability and willingness to sabotage us, above and beyond its IP theft and intelligence theft, but if it does it's not telling us.

But let's take a step back. Since when did we conflate IP theft and the OPM hack? Those are different problems, and I'd really love to have a discussion — which surely wouldn't happen with any government officials in any unclassified forum — whether the OPM hack is now considered a *more* urgent threat than serial Chinese IP theft, or whether Clapper is being honest in

consistently dismissing it as similar behavior to what we do. Sure, IP theft used to be the most urgent issue, but did that change when China absconded with a database of much of our clearance data? The relative urgency of the two seems an utterly critical thing to understand, given that China pwned us in the OPM hack, and now 3 months after discovering that, we're signing a cyber agreement.

All the more so given that the OPM hack goes right to the issue of anonymity though not, perhaps, verifiability.

In his piece, Goldsmith is a bit more trusting of the Clapper claim — which I laid out here — that we lost technical accesses in the wake of the Snowden leaks. I think that may well be the case, but it's just as likely that's disinformation, either for Congress in advance of the Xi Jinping visit, or for the Chinese. Goldsmith presents that as one more reason why we can't verify any agreement, and therefore it will be largely worthless.

But does it matter that the OPM hack created symmetry in transparency of personnel (which is different from technical accesses) between China and the US? Does it matter that, with the OPM hack, the Chinese largely replicated our ability to create fingerprints using XKS, and through that figure out who in China was doing what?

That is, we may not have full attribution ability right now — in Clapper's description it sounded like we could consistently ID tools and persona, but not necessarily tie that persona back to the Chinese state, though, again, that my have been disinformation. But both the US (through XKS) and China (through OPM) have achieved a kind of transparency in personnel.

Which brings me to my central question, in response to Goldsmith's claim this agreement is pretty meaningless because of the attribution and verification problems. He may well be right it will be a mostly symbolic agreement (though if we move towards norms that may be a positive

step).

But until we tease out the real interaction of the old problem — the IP theft — with the new one — that China has our intelligence community by the balls, and until we develop more certainty that some other acts of sabotage aren't, in fact, cyberattacks, I'm not sure we're really understanding the dynamics behind the agreement.

Just as importantly, it seems, we need to understand what a new kind of personnel transparency affects our expectations about verification or trust in cyberspace. I don't know the answer to whether this kind of symmetry chances the considerations on verification or not, but it does seem a relevant question.