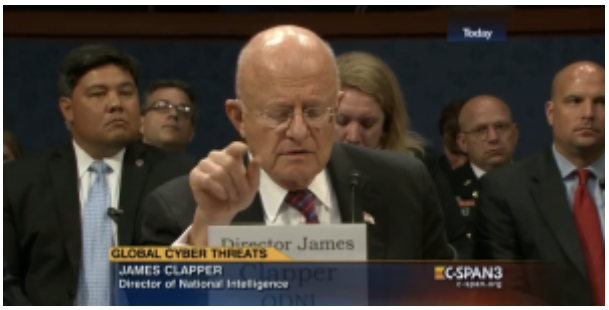
WHAT IF THE INTELLIGENCE COMMUNITY IS LOOKING FOR THE WRONG MALICIOUS USE OF OPM DATA?



The revelation in last week's cyber threats hearing the press has been most agog about is that James Clapper predicted hackers would get around to changing, rather than just stealing, data.

> [after 19:00] In the future I believe we'll see more cyber operations that will change or manipulate electronic information to compromise its integrity – in other words, compromise its accuracy and its reliability, instead of merely deleting it or disrupting access to it.
>
> [snip]
>
> [after 56:00] To this point, it's either been disruption – of a website, for example, but more commonly, just purloining information. As I indicated in my opening statement though, I believe the next push on the envelope here is going to be the manipulation or deletion of data, which will of course compromise its integrity.

Um. Really, journalists who cover this area?

The notion that a cyber operator will change data is not new. Proof of that concept happened years ago, with the StuxNet attack, when US and Israeli hackers made the Iranians think everything was going peachy with their centrifuges when in fact they were spinning out of control. No one may yet have manipulated *our* data, but we've manipulated others' data.

Which I guess means, according to Clapper's definition, StuxNet was an attack and not just a hack — in case you had any doubts.

One thing I found far more interesting was Clapper's repeated assertion that the IC has seen no use of the Office of Personnel Management data.

> [after 49:00; see also after 1:29]
> Clapper: What we've done is speculate how it could be used. And again the distinction I was just making with Congressman Westmoreland had to do with the terminology of saying that the OPM breach was an attack. Getting back to definitional issues, we wouldn't characterize it that way. What's of great concern with respect to the OPM breach, which I spoke to briefly in my opening statement had to do with potential uses of that data. And of course, we're looking. Thus far we haven't seen any evidence of their usage of that data.

I said as I was watching and others have said since that this likely just reflects China — almost universally believed to be the OPM perpetrator — playing the long game. It will use the knowledge when it's good and ready, all the while we'll know it has it.

All that said, the *other* thing Clapper said that I found very interesting was that the IC has varying degrees of confidence about who did this hack.

> [after 20:00] Clapper: And while speaking of the OPM breaches, let me say a couple of words about attribution, which is not a simple process and involves at least three related but distinct determinations: geographic point of origin, the identity of the actual perpetrator doing the keystrokes, and the responsibility for actually directing the attack. In the case of OPM, we've had differing degrees of confidence across the IC in our assessment of the responsibility for each of these elements. Of late, unauthorized disclosures and foreign defensive improvements have cost us some technical accesses.

Apparently, not everyone in the IC is completely convinced China did this. This is the kind of statement we never saw, as far as I remember, with regards to the Sony hack (though, admittedly, it's a lot easier to make unsubstantiated accusations against North Korea than China). Are people really not convinced?

Note, too, the casual reference to the US losing some technical accesses, presumably in response to Snowden's disclosures and the heightened awareness from our adversaries just how badly we've pawned them for years. Given the assumption China hacked OPM, this likely means we've lost some visibility into Chinese actions in the last two years.

The evidence China did this hack in part stems from its complexity; few — but not no — other actors could pull it off. That someone would hack United, in tandem with OPM, would support that, given that United flies so many flights from Dulles to China.

All that said is it possible — remotely — some other sophisticated state actor could have done this?

I'm going to assume Clapper is just downplaying

the certainty here, possibly in advance of Xi Jinping's visit to DC.

But if it is remotely true, would that have an effect on our ability to monitor for the use — or even manipulation — of OPM data? That is, if we were looking for Chinese use of the data — focusing on people of Chinese descent and/or people stationed there — would we miss attempts to compromise clearance holders another sophisticated state actor — say, Israel — might target? I'll just remind that at a time when the US was trying to set up the IRGC for an assassination attempt, someone spamouflaged what likely included our target. I presume that as we got closer and then finalized the Iran deal, Israel's targeting of our spooks has intensified.

In any case, Clapper seems confident that the data was not compromised here, which is something other commentators have raised as a worry (because doing so would allow you to create clearances for people who had not been vetted, for example).

> [after 1:29]My working definition of whether it's an attack or not and my characterization of it not being an attack in that there was no destruction of data or manipulation of data, it was simply stolen.

But if we're not 100% sure this is China (again, I'm skeptical we have much doubt), maybe we couldn't be so sure about whether the data has been manipulated or — at the very least — used to compromise our clearance holders.