IN NYT'S FICTIONAL PRESENTATION, CHINA PIONEERED THE "COLLECT IT ALL" STRATEGY

Way down in the second-to-last paragraph of this NYT piece claiming the US will retaliate against China for the OPM hack, national security reporter David Sanger makes this claim about the hack, about experts affiliated with an agency that aspires to "Collect it all."

> Instead, the goal was espionage, on a scale that no one imagined before.

He follows it — he ends the entire article — with uncritical citation of this statement from a senior intelligence official.

> "This is one of those cases where you have to ask, 'Does the size of the operation change the nature of it?' " one senior intelligence official said. "Clearly, it does."

Several paragraphs earlier, the reporter who did a lot of the most important work exposing the first-of-its-type StuxNet attack makes this claim. (NYLibertarian noted this earlier today.)

> The United States has been cautious about using cyberweapons or even discussing it.

In other words, built into this story, written by a person who knows better, is a fiction about the US' own aggressive spying and cyberwar. Sanger even suggests that the sensors we've got buried in Chinese networks exist solely to warn of attacks, and not to collect information just like that which China stole from OPM.

So if someone creating either a willful or lazy fiction also says this …

> That does not mean a response will happen anytime soon — or be obvious when it does. The White House could determine that the downsides of any meaningful, yet proportionate, retaliation outweigh the benefits, or will lead to retaliation on American firms or individuals doing work in China. President Obama, clearly seeking leverage, has asked his staff to come up with a more creative set of responses.

… We'd do well to ask whether this is nothing more than propaganda, an effort to dissipate calls for a more aggressive response from Congress and others.

There is, however, one other underlying potential tension here. Yesterday, Aram Roston explained why some folks who work at NSA may be even more dissatisfied then they were when a contractor exposed their secrets for the world to see.

> Employees at the National Security Agency complain that the director, Adm. Michael Rogers, is neglecting the intelligence agency in favor of his other job, running the military's Cyber Command, three sources with deep knowledge of the NSA have told BuzzFeed News.
>
> "He's spending all his time at CYBERCOM," one NSA insider said. "Morale is bad because of a lack of leadership." A second source, who is close to the agency, agreed that employees are complaining that Rogers doesn't seem to focus on leading the agency. A third said "there is that vibe going on. But I don't know if it's true."
>
> [snip]

> [O]ne of the NSA sources said Rogers appears to be focusing on CYBERCOM not just because the new organization is growing rapidly but also because it has a more direct mission and simpler military structure than the complex and scandal-ridden NSA in its post-Snowden era. That makes focusing on CYBERCOM easier, that source said, "than trying to redesign the National Security Agency."

If true (note one of Roston's sources suggests it may not be), it suggests one of the most important advisors on the issue of how to respond to China's pawning the US is institutionally limiting his focus to his offensive role, not on his information collection (to say nothing of defensive) role. So if Roston's sources are correct, we are in a *very* dangerous position, having a guy who is neglecting other potential options drive the discussion about how to respond to the OPM hack.

And there's one detail in Sanger's story that suggests Roston's sources may be right — where Rogers describes "creating costs" for China, but those costs consist of an escalation of what is, in fact, a two-sided intelligence bonanza.

> Admiral Rogers stressed the need for "creating costs" for attackers responsible for the intrusion,

Those of us without the weapons Rogers has at his disposal think of other ways of "creating costs" — of raising the costs on the front end, to make spies adopt a more targeted approach to their spying. Those methods, too, might be worth considering in this situation. If we're going to brainstorm about how to deal with the new scenario where both the world's major powers have adopted a bulk collection approach, maybe the entire world would be safer thinking outside the offensive weapon box?