US GETTING ITS CYBER-ASS HANDED TO IT

David Sanger has early reporting on a report that will be sure to affect the NSA debate, though it has nothing to do with Edward Snowden. The National Commission for the Review of the Research and Development Programs of the United States Intelligence Community, which has been reviewing our cybercapabilities for two years, has found that we're losing any edge we have.

The problems?

- [In-Q-Tel founder Gilman] Louie also said the intelligence agencies were heavily focused on the development of offensive cyberweapons because "it is easier and more intellectually interesting to play offense than defense." "Defense is where we are losing the ballgame," he said.
- The leader of science and technology for [the Director of National Intelligence] office, commission members said Tuesday, was not aware of some of the most classified research and development programs. They also found that intelligence agencies were duplicating efforts by pursuing similar projects at the same time, but because operations were

compartmentalized, few researchers were aware of their colleagues' work.

- Shirley Ann Jackson, the president of Rensselaer Polytechnic Institute, found particular fault with the intelligence agencies' approach, "which involves gathering more data than you need."

Again, these panel members have come to this conclusion completely independent of the Snowden revelations, but they should well fuel the very questions his disclosures have been driving, because they, like Snowden, show that aggressive Big Data badly organized won't keep our country safe.

In related news, there are reports that NSA will be reorganized with Keith Alexander's departure, by splitting of CYBERCOM from NSA.

> Senior military officials are leaning toward removing the National Security Agency director's authority over U.S. Cyber Command, according to a former high-ranking administration official familiar with internal discussions.
>
> [snip]
>
> No formal decision has been made yet, but the Pentagon has already drawn up a list of possible civilian candidates for the next NSA director, the former official told The Hill. A separate military officer would head up Cyber Command, a team of military hackers that trains for offensive cyberattacks and protects U.S. computer systems.

I think this is the wrong solution (and the anonymous leaks here sound as much like Generals

trying to make a bid for turf as it does a real decision).

One of several big problems with our cyber stature is that there is no champion for defending (rather than policing) the US. That means we've committed to the same kind of approach we use with terrorists, trying to inflame terrorists we've found hints of so we can demobilize them, rather than just trying to harden our vulnerabilities to make it very difficult or unrewarding to attack.

And in inflaming and spying, we've been relying on weakening security, so we can see them, which makes the cyberattackers' job easier.

Moreover there are a lot more real cyberattackers than real terrorists out there, and they can do far more damage than any but the very lucky 9/11 team could pull off. Which means if you miss here, you miss big. Whereas if we spent money on defense, we might be better able to withstand these attacks.

So I still say we need a very well-funded cyberdefense entity (I said put it in DHS, not because DHS is functional, but because that agency should but doesn't operate under a different paradigm) that will be held responsible for successful attacks.