STEPHEN CAMBONE, HACKER PWN, USED TO HEAD DOD'S "INTELLIGENCE"

Stephen Cambone was the first ever Under Secretary of Defense for something called "Intelligence."

In that role, he oversaw a domestic spying program that targeted hippies and made GOP cronies rich. And then he went on to profit off that domestic spying program at a company called QinetiQ.

Which is why I'm having a hard time summoning much grief that Chinese hackers have pwned another US Defense Contractor — none other than QinetiQ (George Tenet, another noted "intelligence" figure, was there until 2008)!

Here are the kinds of things the hackers accessed, almost unimpeded.

> The lengthy spying operation on QinetiQ jeopardized the company's sensitive technology involving drones, satellites, the U.S. Army's combat helicopter fleet, and military robotics, both already-deployed systems and those still in development, according to internal investigations.

And here is the kind of access QinetiQ allowed both Chinese and Russian hackers.

> In 2008, a security team found that QinetiQ's internal corporate network could be accessed from a Waltham, Massachusetts, parking lot using an unsecured Wi-Fi connection. The same investigation discovered that Russian hackers had been stealing secrets from QinetiQ for more than 2 1/2 years through a secretary's computer, which

> they had rigged to send the data directly to a server in the Russian Federation, according to an internal investigation.

Read the whole thing – you won't know whether to laugh or cry.

Meanwhile, the government seems more intent on violating my privacy to fix this kind of wholesale hacking, rather than blackballing those contractors who are incapable of securing their networks.

> The State Department, which has the power to revoke QinetiQ's charter to handle restricted military technology if it finds negligence, has yet to take any action against the company.
>
> [snip]
>
> In May 2012, QinetiQ received a $4.7 million cyber-security contract from the U.S. Transportation Department, which includes protection of the country's critical transport infrastructure.

The same company that let China hack at will for years is being paid millions for cybersecurity.

That about says it all.