DID CHINA AND RUSSIA REALLY NEED OUR HELP TARGETING SPOOK TECHIES?

LAT has a story describing what a slew of others — including me — have already laid out. The OPM hack will enable China to cross-reference a bunch of databases to target our spooks. Aside from laying all that out again (which is worthwhile, because not a lot of people are still not publicly discussing that), LAT notes Russia is doing the same.

But other than that (and some false claims the US doesn't do the same, including working with contractors and "criminal" hackers) and a review of the dubiously legal Junaid Hussain drone killing, LAT includes one piece of actual news.

> At least one clandestine network of American engineers and scientists who provide technical assistance to U.S. undercover operatives and agents overseas has been compromised as a result, according to two U.S. officials.

I would be unsurprised that China was rolling up actual HUMINT spies in China as a result of the OPM breach (which would explain why we'd be doing the same in response, if that's what we're doing). But the LAT says China (and/or Russia) is targeting "engineers and scientists who provide technical assistance" to spooks — one step removed from the people recruiting Chinese (or Russian) nationals to share its country's secrets.

I find that description rather curious because of the way it resembles the complaint by CIA contractor whistleblower John Reidy in an appeal of a denial of a whistleblower complaint by CIA's Inspector General. (Marisa Taylor first reported on Reidy's case.) As I extrapolated

from redactions some weeks ago, it looks like Reidy reported CIA's reporting system getting hacked at least as early as 2007, but the contractors whose system got (apparently) hacked got him fired and CIA suppressed his complaints, only to have the problem get worse in the following years until CIA finally started doing something about it — with incomplete information — starting in 2010.

> Reidy describes playing three roles in 2005: facilitating the dissemination of intelligence reporting to the Intelligence Community, identifying Human Intelligence (HUMINT) targets of interest for exploitation, and (because of resource shortages) handling the daily administrative functions of running a human asset. In the second of those three roles, he was "assigned the telecommunications and information operations account" (which is not surprising, because that's the kind of service SAIC provides to the intelligence community). In other words, he seems to have worked at the intersection of human assets and electronic reporting on those assets.
>
> Whatever role he played, he described what by 2010 had become a "catastrophic intelligence failure[]" in which "upwards of 70% of our operations had been compromised." The problem appears to have arisen because "the US communications infrastructure was under siege," which sounds like CIA may have gotten hacked. At least by 2007, he had warned that several of the CIA's operations had been compromised, with some sources stopping all communications suddenly and others providing reports that were clearly false, or "atmospherics" submitted as solid reporting to fluff reporting numbers. By 2011 the government had appointed a Task Force to deal with the problem he had

> identified years earlier, though some on that Task Force didn't even know how long the problem had existed or that Reidy had tried to alert the CIA and Congress to the problem.
>
> All that seems to point to the possibility that tech contractors had set up a reporting system that had been compromised by adversaries, a guess that is reinforced by his stated desire to bring a "*qui tam* lawsuit brought against CIA contractors for providing products whose maintenance and design are inherently flawed and yet they are still charging the government for the products." In his complaint, he describes Raytheon employees being reassigned, suggesting that contracting giant may be one of the culprits, but all three named contractors (SAIC, Raytheon, and Mantech) have had their lapses; remember that SAIC was the lead contractor that Thomas Drake and friends exposed.

Reidy's appeal makes it clear that one of the things that exacerbated this problem was overlapping jurisdiction, with a functional unit apparently taking over control from a geographic unit. While that in no way rules out China, it sounded as much like the conflict between CIA's Middle East and Counterterrorism groups that has surfaced in other areas as anything else.

The reason I raise Reidy is because — whether or not the engineers targeted as described in the LAT story are the same as the ones Reidy seems to describe — Reidy's appeal suggests the problem he described *arose from contractor incompetence and cover-ups*.

I guess you could say the same about the OPM hack (though it was also OPM's incompetence). Except in the earlier case, you're talking far more significant intelligence contractors — including SAIC and Raytheon, who both do a lot

of cybersecurity contracting on top of their intelligence contracting — and a years-long cover up with the assistance of the agency in question.

All while assets were being exposed, apparently because of insecure computer systems.

China's hacking is a real threat to the identities of those who recruit human sources (and therefore of the human sources themselves).

But if Reidy's complaint is true, then it's not clear how much work China really needs to do to compromise these identities.