CONFIRMED: LISTENING TO WHISTLEBLOWER JOHN REIDY COULD HAVE SAVED THE LIVES OF NUMEROUS CIA ASSETS

Back in 2015, I looked at the whistleblower case of John Reidy, a former CIA contractor who had warned of catastrophic failures in a communications system.

> 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,

When news of CIA's loss of numerous Chinese assets came out, I again pointed back to Reidy's warnings.

Today, Yahoo confirms that the communications system weakness first identified by Reidy 11 years ago was indeed exploited first by Iran (where, Yahoo says, Reidy was stationed), then by China, and to a lesser degree, Russia.

Iran was able to use the vulnerability to unwind the US' network of spies by using Google to identify signatures of the system.

> This hunt for CIA sources eventually bore fruit — including the identification of the covert communications system.
>
> A 2011 Iranian television broadcast that touted the government's destruction of the CIA network said U.S. intelligence operatives had created websites for fake companies to recruit agents in Iran by promising them jobs, visas and education abroad. Iranians who initially thought they were responding to legitimate opportunities would end up meeting with CIA officers in places like Dubai or Istanbul for recruitment, according to

> the broadcast.
>
> Though the Iranians didn't say precisely how they infiltrated the network, two former U.S. intelligence officials said that the Iranians cultivated a double agent who led them to the secret CIA communications system. This online system allowed CIA officers and their sources to communicate remotely in difficult operational environments like China and Iran, where in-person meetings are often dangerous.
>
> A lack of proper vetting of sources may have led to the CIA inadvertently running a double agent, said one former senior official — a consequence of the CIA's pressing need at the time to develop highly placed agents inside the Islamic Republic. After this betrayal, Israeli intelligence tipped off the CIA that Iran had likely identified some of its assets, said the same former official.
>
> The losses could have stopped there. But U.S. officials believe Iranian intelligence was then able to compromise the covert communications system. At the CIA, there was "shock and awe" about the simplicity of the technique the Iranians used to successfully compromise the system, said one former official.
>
> In fact, the Iranians used Google to identify the website the CIA was were using to communicate with agents. Because Google is continuously scraping the internet for information about all the world's websites, it can function as a tremendous investigative tool — even for counter-espionage purposes. And Google's search functions allow users to employ advanced operators — like "AND," "OR," and other, much more sophisticated ones — that weed out and isolate websites and online data with extreme

> specificity.
>
> According to the former intelligence official, once the Iranian double agent showed Iranian intelligence the website used to communicate with his or her CIA handlers, they began to scour the internet for websites with similar digital signifiers or components — eventually hitting on the right string of advanced search terms to locate other secret CIA websites. From there, Iranian intelligence tracked who was visiting these sites, and from where, and began to unravel the wider CIA network.

Yahoo describes that Iran and China likely traded technology, which is how China proceeded to use the same technique to target CIA assets.

While Yahoo doesn't emphasize it, it seems likely that if SAIC and Raytheon hadn't had so much power when Reidy first started warning of this compromise, it would have been addressed far more quickly. Instead, he lost clearance and was fired.

Which, on top of a lot of other lessons, seems to be a superb example of how ignoring a whistleblower can have catastrophic consequences.