WERE SHITTY SAIC SYSTEMS THE CAUSE OF THE CIA'S CHINA DISASTER?

The NYT has a story about how China started rolling up CIA's spy network in 2010, the cause of which (the story says) still has not been solved. One possible cause is that a Chinese-American exposed America's spies to the Chinese. But the government was never able to establish enough proof that he was the Chinese mole to arrest him, not even when they lured him back to the US to try to bust him.

> The mole hunt eventually zeroed in on a former agency operative who had worked in the C.I.A.'s division overseeing China, believing he was most likely responsible for the crippling disclosures. But efforts to gather enough evidence to arrest him failed, and he is now living in another Asian country, current and former officials said.
>
> [snip]
>
> As investigators narrowed the list of suspects with access to the information, they started focusing on a Chinese-American who had left the C.I.A. shortly before the intelligence losses began. Some investigators believed he had become disgruntled and had begun spying for China. One official said the man had access to the identities of C.I.A. informants and fit all the indicators on a matrix used to identify espionage threats.
>
> After leaving the C.I.A., the man decided to remain in Asia with his family and pursue a business opportunity, which some officials

> suspect that Chinese intelligence agents had arranged.
>
> Officials said the F.B.I. and the C.I.A. lured the man back to the United States around 2012 with a ruse about a possible contract with the agency, an arrangement common among former officers. Agents questioned the man, asking why he had decided to stay in Asia, concerned that he possessed a number of secrets that would be valuable to the Chinese. It's not clear whether agents confronted the man about whether he had spied for China.
>
> The man defended his reasons for living in Asia and did not admit any wrongdoing, an official said. He then returned to Asia.

A second possibility is that bad tradecraft allowed China to discover America's spies.

> Those who rejected the mole theory attributed the losses to sloppy American tradecraft at a time when the Chinese were becoming better at monitoring American espionage activities in the country. Some F.B.I. agents became convinced that C.I.A. handlers in Beijing too often traveled the same routes to the same meeting points, which would have helped China's vast surveillance network identify the spies in its midst.
>
> Some officers met their sources at a restaurant where Chinese agents had planted listening devices, former officials said, and even the waiters worked for Chinese intelligence.

A third possibility — which the NYT doesn't examine at length and which it ties to the poor tradecraft — is that China hacked the CIA's method of communicating with assets.

> Others believed that the Chinese had hacked the covert system the C.I.A. used to communicate with its foreign sources.
>
> [snip]
>
> Some investigators believed the Chinese had cracked the encrypted method that the C.I.A. used to communicate with its assets.
>
> [snip]
>
> This carelessness, coupled with the possibility that the Chinese had hacked the covert communications channel, would explain many, if not all, of the disappearances and deaths, some former officials said.

I lay these three possibilities out because the timing of the moment the exposure became critical — 2010 and 2011 — and the allusions to a hacked covert communication channel sound a lot like what CIA whistleblower John Reidy complained about seeing his employer, SAIC, oversee starting in 2005. While his complaint is heavily redacted, it sounded like he accused SAIC of providing inadequate security for a system serving the intersection of human assets and electronic reporting.

> [H]is heavily redacted appeal at least appears to suggest his complaint was very serious and should have been a timely way to limit the compromise of CIA assets and officers.
>
> 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. [my emphasis]
>
> 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."

The task force described in Reidy's complaint coincides with the "Honey Badger" investigation described in the NYT, and the scale of the losses – 70% of operations compromised – sounds the same too. Reidy complained that those working on the task force didn't learn how long he had been calling attention to the problem. And as he was appealing his complaint, he was being spied on by the intelligence community.

Of course, Reidy's complaints were especially easy to silence because he was a contractor that the intelligence contractor community basically blacklisted.

I'm checking with the NYT reporters to see if this sounds like their story. But either the CIA had two catastrophic intelligence failures at the same time in 2010, or this sounds like the Chinese compromise.

In which case the fourth possibility to explain the compromise is that shitty intelligence contractors created the problem and then covered it up.