NORTH KOREA AND SONY: JAMES CLAPPER DESCRIBES HIS TRIP

As debates about whether North Korea hacked Sony continue (or even better, websites mockingly show you could randomly assign blame to any number of people; h/t Kim Zetter), there's something that has long bothered me. The excuse for the government's failure to provide a more fulsome description of the reasons it is so sure North Korea is to blame always go back to (NSA's) sources and methods.

For example, here's Jack Goldsmith making the legitimate argument that one reason you can't attribute properly is because it would expose what we don't know, and make us more vulnerable to hackers.

> The problem with saying that the "secrecy of the NSA's sources and methods is going to have to take a back seat to the public's right to know" is that public knowledge could exacerbate the cyber threat. For when other countries know those aspects of those sources and methods, they can hide their tracks better in the next attack. The U.S. Government might think that the credibility hit it takes for not revealing more in the face of this relatively mild attack on Sony is outweighed by the longer-term advantages — to meeting and defeating greater cybersecurity threats — of having penetrated networks and conversations in unknown ways. The game is iterative, and the proper balance of secrecy and disclosure at any particular time is tricky.

There's one part of the hack, however, for which such claims can't be made — and which, in the

government's descriptions, has been just as weak as the FBI's public forensic case against North Korea: motive.

Not only did the movie *The Interview*, only become the motive well after the hack, but — even assuming Kim Jong-Un is batshit crazy — the rest of the hack still doesn't make sense. Why burn all those stars before targeting *The Interview*? Why release so much about Sony's IP and other financial dealings before targeting *The Interview*? Why do nothing in the face of *The Interview*'s subsequent release and broad success? In other words, why does the bulk of the attack actually not attack the purported target of it? Heck, the hackers didn't even make the most of the materials on the *Interview* obtained in the hack to best serve North Korea's interests.

No description of the motive I've seen makes any sense (again, even assuming that everyone in North Korean positions of authority are crazy or at least irrational).

Meanwhile, as far as I know I had been the only person to point out that James Clapper made a highly unusual trip to North Korea just weeks before the hack to pick up two Americans North Korea claims were US spies.

> Curiously, claims that North Korea launched the hack make no mention of James Clapper's highly unusual trip to North Korea, just a few weeks before the hack was discovered, to pick up two Americans North Korea had imprisoned, claiming they were spies.

It seems to me you might more likely find a rational motive for a rash attack on US soil (albeit at the US subsidiary of Japanese company) in that trip than in a movie, no matter how curious the movies' ties to US national security figures. That is, not only did North Korea allegedly hack Sony for a movie reviewed by government officials depicting the

assassination of Kim, but it did so weeks after the top US spy personally flew to North Korea to rescue two Americans North Korea claimed were spies, one of whom entered on a tourist visa and then ripped it up claiming he wanted to talk to North Koreans.

Reports from a press blitz Clapper did upon his return described Clapper delivering a letter from President Obama — which he described as doing no more than naming Clapper as envoy to pick up the two Americans but which Clapper declined to quote — and North Korea as disappointed that Obama hadn't offered something more in exchange for the prisoners.

> Mr. Clapper revealed details of the trip in an interview with The Wall Street Journal. The North Koreans seemed disappointed when he arrived without a broader peace overture in hand, he said. At the same time, they didn't ask for anything specific in return for the prisoners' release.
>
> U.S. officials say the mission, which few officials within the Obama administration knew about until Mr. Clapper was returning, wasn't meant to signal any change in the U.S.'s approach to the reclusive North.
>
> Mr. Clapper's earlier conversations with older North Korean officials on his one-day trip had been contentious. He heard what he called a far more "tempered" tone from a younger North Korean whom he described as an interlocutor and who accompanied him on the 40-minute drive back to the airport at the trip's end. He said the interlocutor expressed regret that the North and South remained split and asked Mr. Clapper if he'd return to Pyongyang.
>
> [snip]
>
> The plan to send Mr. Clapper came together suddenly.

> North Korea made clear that it wanted the U.S. to send a “senior envoy” and that it wanted a communication from the president.
>
> The White House tapped Mr. Clapper, because he was a cabinet-level official though not a member of the cabinet or a diplomat. The White House didn’t want to signal to the North Koreans that Mr. Clapper was being sent to conduct a diplomatic negotiation. Mr. Clapper had also served as a military intelligence officer in South Korea in the mid-1980s and had a continuing interest in the Korean peninsula.
>
> [snip]
>
> Gen. Kim Young Chol appeared to be taken aback when handed the letter, Mr. Clapper said.
>
> Written in English, the letter introduced Mr. Clapper as the president’s envoy and “characterized the release of the two detainees as a positive gesture,” Mr. Clapper said, declining to quote it directly. “It didn’t apologize.”

It’s possible there was more to the trip than Clapper’s very boisterous press blitz let on.

And it turns out I’m no longer the only one who links the trip to North Korea and the hack. At a speech at a cybersecurity conference at Fordham today, Clapper repeated accusations that North Korea had done the Sony hack, claiming that the General Kim Youn(g) Chol, with whom he had met on his trip, ordered the attack (see also Eamon Javers’ TL) amid more details of what went wrong with his plane and other details of his trip. The Bureau Kim Youn(g) Chol heads is among those sanctioned last week in response to the hack, though it doesn’t appear he’s among the sanction targets himself (though there is someone with a very similar name, Kim Yong Chol,

who is Korea Mining Company's representative in Iran, who was sanctioned).

I'm still not convinced that North Korea did the hack. But if they did, then there's more of a backstory, precisely where Clapper is pointing to it: in his trip to North Korea just weeks before the hack.

Alternately, Clapper's fixation on his trip may suggest his meeting with Kin Youn(g) Chol has influenced analysis of the hack, leading Clapper's subordinates to ascribe more importance to heated meetings while their boss was in North Korea than they logically should.

Either way, Clapper's giving a very partial description of that trip. But now that he has returned to doing so, it ought to be a much more significant focus for reporting on the alleged North Korea hack.