IF IPS ARE SO SOLID, WHY WON'T FBI TELL US HOW MANY AMERICANS GET SUCKED UP IN SECTION 702?

By his own admission, James Clapper had dinner with the North Korean General who (again, according to Clapper) ordered the hack on Sony just weeks before the hack happened. That puts him at most two degrees away from the actual hackers, according to the evidence presented by Clapper and Jim Comey. According to the Intelligence Community's at times naive analytical game of Three Degrees of Osama bin Laden — one which has repeatedly targeted negotiators like Clapper was in November, rather than culprits — Clapper should be sanctioned along with all the others President Obama has targeted.

…

…

That is, of course, absurd. We know James Clapper. And while his word may have not *much* more credibility at this point than Kim Jong-Un's, that doesn't mean his effort to negotiate a hostage release (and whatever else he and North Korea believed was being discussed at the time) makes him a culprit in the hack.

But I think the thought experiment provides useful background to consideration of Comey's further explanation — littered with infantilizing language about bad guys and the "very dark jobs" of FBI's behavioral analysts who "profile bad actors" — of why he and the rest of the Intelligence Community is so certain North Korea, the country, did the Sony hack.

Comey says the data deletion used in the hack was used by "the North Koreans" in the past (his

conflation of “North Koreans” and “North Korea” continues throughout).

> You know the technical analysis of the data deletion malware from the attack shows clear links to other malware that we know the North Koreans previously developed. The tools in the Sony attack bore striking similarities to another cyber attack the North Koreans conducted against South Korean banks and media outlets. We’ve done a—I have, as you know from watching Silence of the Lambs—about people who sit at Quantico, very dark jobs. Their jobs are to try to understand the minds of bad actors. That’s our behavioral analysis unit. We put them to work studying the statement, the writings, the diction of the people involved claiming to be the so-called guardians of peace in this attack and compared it to other attacks we know the North Koreans have done. And they say, “Easy. For us it’s the same actors.”

(See Errata for some nuance about that claim.)

Comey then explained how the IC (but not outside skeptics) red teamed the IC’s own conclusions.

> We brought in a red team from all across the intelligence community and said let’s hack at this. What else could be explaining this? What other explanations might there be? What might be missing? What competing hypotheses might there be? Evaluate possible alternatives—what might be missing? And we ended up in the same place.

Then, before Comey admitted that FBI still doesn’t know how “the North Koreans” hacked their way into Sony, Comey offered this detail to rebut the outside skeptics’ concerns.

> Now I know because I’ve read in the newspaper—seen in the news—that some

> serious folks have suggested that we have it wrong. I would suggest—not suggesting, I'm saying—that they don't have the facts that I have—don't see what I see—but there are a couple things I have urged the intelligence community to declassify that I will tell you right now.
>
> The Guardians of Peace would send e-mails threatening Sony employees and would post online various statements explaining their work. And in nearly every case they used proxy servers to disguise where they were coming from. And sending those e-mails and then sending and pasting and posting those statements.
>
> And several times they got sloppy. Several times either because they forgot or because they had a technical problem they connected directly and we could see them. And we could see that the IP addresses being used to post and to send the e-mails were coming from IPs that were exclusively used by the North Koreans. It was a mistake by them that we haven't told you about before that was a very clear indication of who was doing this. They shut it off very quickly once they realized the mistake. But not before we knew where it was coming from.

That is, Comey's new tell — which has, with apparent other leaking about a Facebook account from Mandiant, gotten headlines — is that the FBI identified the hackers using "IPs that were exclusively used by *the North Koreans*." [my emphasis]

Let me interject here and remind you that NSA and the FBI refuse to count how many US persons get sucked up in Section 702 upstream and PRISM collection because IPs aren't a reliable indicator of the location of a person.

The USA Freedom Act, by law, excluded any consideration of IP (frankly, any consideration of Internet location at all) from its obligation to report on the location of people sucked up in the dragnet. According to the FBI, tracking location based off anything but a (US based) phone number is too onerous for the Bureau.

IP is unreliable when it comes to transparency on the FBI, but rock solid when it comes to claims of attribution.

Now, I admit that's a very different thing than spending months and years tracking one IP and attributing it to one particular actor.

But as Jeffrey Carr notes, even there the FBI's claims have problems. He points out that the claims Comey made yesterday are remarkably similar to those used to attribute the Dark Seoul attack in 2013.

> This sounded remarkably similar to the mistake made by the alleged North Korean hackers in the Dark Seoul attack of March 2013:
>
> > *"SEOUL – A technical blunder by a hacker appears to have reinforced what South Korea has long suspected: North Korea has been behind several hacking attacks on South Korea in recent years…. The hacker exposed the IP address (175.45.178.xx) for up to several minutes due to technical problems in a communication network, giving South Korea a rare clue into tracing the origin of the hacking attack that took place on March 20, according to South Korean officials."*
>
> The evidence that the FBI believes it has against the DPRK in the Sony attack stems from the data that it received on the Dark Seoul attack last year from the

> private sector.

He then notes North Korea's Internet isn't as locked down as it was just a few years ago — and one possible point of entry is geographically close to the St. Regis Hotel increasingly pinpointed in such attacks.

> However the easiest way to compromise a node on North Korea's Internet is to go through its ISP — Star Joint Venture. Star JV is a joint venture between North Korea Post and Telecommunications Corporation and another joint venture — Loxley Pacific (Loxpac). Loxpac is a joint venture with Charring Thai Wire Beta, Loxley, Teltech (Finland), and Jarungthai (Taiwan).
>
> I explored the Loxley connection as soon as this story broke, knowing that the FBI and the NSA was most likely relying on the myth of a "closed" North Korean Internet to base their attribution findings upon. Loxley is owned by one of Thailand's most well-connected families and just 4 kilometers away is the five star St. Regis hotel where one of the hackers first dumped Sony's files over the hotel's WiFi. It would be a simple matter to gain access to Loxley's or Loxpac's network via an insider or through a spear phishing attack and then browse through NK's intranet with trusted Loxpac credentials.
>
> Once there, how hard would it be to compromise a server? According to HP's North Korea Security Briefing (August 2014) it would be like stealing candy from a baby.

Now, none of that proves the FBI is wrong (just as none of it, without more proof, is enough to unquestioningly believe the FBI). I frankly am a lot more interested in what went on in Clapper's

meeting right now than I am in IP claims without more proof.

But if the FBI is going to claim that IP is a rock solid indicator of someone's ID, then can it also tell us how many Americans it sucks up into the dragnet?