WHITHER SHADOW BROKERS IN DISCUSSIONS OF FOREIGN HACKS OF AMERICA?

Since Shadow Brokers first started leaking apparent NSA tools in August, there have been very few mentions of the compromise from Congress. Adam Schiff expressed some concern about the compromise at the time (though not about the failures of the Vulnerabilities Equities Process the leaks appeared to indicate). And the HPSCI report on Edward Snowden had a sentence stating, "Recent security breaches at NSA underscore the necessity for the agency to improve its security posture," though that reference doesn't name Hal Martin, the still unnamed NSA TAO employee who stole some hacking tools in 2015 referred to in a November WaPo article, or Shadow Brokers (which may or may not have relied on Martin as a source).

That silence continued today in the Senate Armed Services Committee on Foreign Cyber Threats to the US. Even if Shadow Brokers is not a Russian group, as many people speculated back in August, or even foreign, wouldn't the exposure of NSA's (dated) hacking tools pose a cyber threat by itself?

But there were two exchanges in the hearing that may have pointed to Shadow Brokers. Even if they did not, both are worth bookmarking for the assertions made. In the first exchange, Tom Cotton (who, in addition to SASC, is also on

SSCI, so would be privy to any Shadow Brokers information shared with the full intelligence committees) tried to narrowly bracket what the IC means when it refers to Russia hacking the US (after 1:24).

> Cotton: We've heard a lot of imprecise language here today and it's been in the media here as well. Phrases like "hacked the election," "undermine democracy," "intervened in election." So I want to be more precise here. Director Clapper let's go to the October 7 statement. That says, quote, "the recent compromises of emails from US persons and institutions including from US political organizations" was directed by the Russian government." Are we talking there specifically about the hack of the DNC and the hack of John Podesta's emails?
>
> Clapper: Yes.
>
> Cotton: Are we talking about anything else?
>
> Clapper: That was, *essentially at the time*, what we were talking about.
>
> Cotton: At the time then – it says that "recent disclosures through websites like DC Leaks and Wikileaks … are consistent with the methods and motivations of Russian directed efforts." DNC emails were leaked first, I believe, in July. Is that what the statement is talking about there?
>
> Clapper: I believe so.
>
> Cotton: Mr. Podesta's emails were not leaked I believe until that very day on October 7, so was the statement referring to that, yet, or was that not intending to be included?
>
> Clapper: I'd have to research the exact chronology of when John Podesta's emails

> were compromised. But I think though that that bears on my statement that our assessment now is even more resolute than it was with that statement on the 7th of October. [my emphasis]

Cotton's statement is odd in any case. He makes no mention of the DCCC, which of course had also been hacked by October 7. Moreover, in his second citation from the DHS/ODNI statement, he omits the reference to the Guccifer 2 persona, who leaked the DCCC documents as well as some DNC files and — according to him, at least — handed those over to Wikileaks. So in his effort to inject precision into this discussion, he's either introducing imprecision, or he's revealing details from classified briefings.

In any case, in response to Cotton's questions, Clapper admits that the only hack referenced in the October 7 statement (though it's clear he doesn't have these facts ready at hand). But then he suggests — without much emotion — that what the IC was talking about on October 7 is different from what the IC might include now, which is one reason the IC is more "resolute" about its assessment of Russian attribution.

There are many things Clapper might include in additional entities, not least GOP targets, including Colin Powell (whose emails, after all, had already been released on DC Leaks). One of those is Shadow Brokers.

Fifteen minutes later (after 1:41), Joe Donnelly ask a question that Clapper justifiably can't make sense of.

> The government has named those responsible for the DNC hack as APT 28 and APT 29, part of the Russian intelligence services: the GRU and the FSB. Are all the actors targeted by these two entities known to the public, sir?
>
> Clapper: I'm sorry sir, the question again, are all what?

> Donnelly: All the actors targeted by these two entities, GRU, FSB, APT 28, 29, do we know everybody, have you told us who's involved or are there more that you can't discuss at this time?
>
> Clapper: Right. I don't think I can discuss that in this forum.

It *appears* Donnelly is asking about whether APT 28 and 29 hacked other victims (though when I heard this in real time it sounded like Donnelly was asking about other Russian participants in the hacking). We know they have (indeed, the Joint Analysis Report released the other day discusses those other targets, so they can't be classified at all). But whatever Clapper took from Donnelly's question, he took the answer to be too sensitive to respond to in open session. Furthermore, he said he could not discuss it *in this forum*, not that Donnelly should wait until next week's report.

The Shadow Brokers is still out on Twitter, bitching (as recently as January 1) they didn't get included in the JAR report or sanctions list, suggesting they at least want you to believe they're part of the larger Russian hack.

So why was there no mention of them in the SASC hearing?

Update, 1/10: Embarrassing whither/wither typo fixed. H/t Christopher.