WHAT WAS THE RELATIONSHIP BETWEEN FSB AND GRU IN THE DNC HACK, REDUX?

I want to return to last week's House Intelligence Hearing on Russia (because that fecker Devin Nunes canceled my birthday hearing with James Clapper and John Brennan today), to revisit a question I've asked a number of times (in most detail here): what was the relationship between Russia's FSB and GRU intelligence services in the DNC hack?

The public narrative (laid out in this post) goes like this: Sometime in summer 2015, APT (Advanced Persistent Threat) 29 (associated with FSB, Russia's top intelligence agency) hacked the DNC along with 1,000 other targets and because DNC ignored FBI's repeated warnings, remained in their network unnoticed. Then, in March 2016, APT 28 (generally though not universally associated with GRU, Russia's military intelligence) hacked DNC and John Podesta. According to the public story, GRU oversaw the release (via DC Leaks and Guccifer 2.0) and leaking (to Wikileaks via as-yet unidentified cut-outs) of the stolen documents.

Under the public story, then, FSB did the same kind of thing the US does (for example, with Enrique Peña Nieto in 2012), collecting intelligence on a political campaign, whereas GRU did something new (though under FBI-directed Sabu, we did something similar to Bashar al-Assad in 2012), leaking documents to Wikileaks.

Obama's sanctions to retaliate for the hack primarily focused on GRU, but did target FSB as well, though without sanctioning any FSB officers by name. And in its initial report on the Russian hack, the government conflated the two separate groups, renaming attack tools previously dubbed Cozy and Fancy Bear the

"Grizzly Steppe," making any detailed discussion of how they worked together more confusing. As I noted, however, the report may have offered more detail about what APT 29 did than what APT 28 did.

Last week's hearing might have been an opportunity to clarify this relationship had both sides not been interested in partisan posturing. Will Hurd even asked questions that might have elicited more details on how this worked, but Admiral Mike Rogers refused to discuss even the most basic details of the hacks.

> HURD: Thank you, Chairman.
>
> And gentlemen, thank you all for being here. And thank you for your continued service to your country. I've learned recently the value of sitting in one place for a long period of time and listening and today I'm has added to that understanding and I'm going to try to ask questions that y'all can answer in this format and are within your areas of expertise. And Director Rogers, my first question to you – the exploit that was used by the Russian's to penetrate the DNC, was it sophisticated? Was it a zero day exploit? A zero day being some type of – for those that are watching, an exploit that has never been used before?
>
> ROGERS: In an open unclassified forum, I am not going to talk about Russian tactics, techniques or procedures about how they executed their hacks.
>
> HURD: If members of the DNC had not – let me rephrase this, can we talk about spear fishing?
>
> ROGERS: Sure, in general terms, yes sir.
>
> HURD: Spear fishing is when somebody sends an email and they – somebody clicks on something in that email…

> ROGERS: Right, the user of things (inaudible) they're receiving an email either of interest or from a legitimate user, they open it up and they'll often click if you will on a link – an attachment.
>
> HURD: Was that type of tactic used in the…
>
> ROGERS: Again, I'm not in an unclassified forum just not going to be…

The refusal to discuss the most basic details of this hack – even after the government listed 31 reports describing APT 28 and 29 (and distinguishing between the two) in its updated report on the hacks – is weird, particularly given the level of detail DOJ released on the FSB-related hack of Yahoo. Given that the tactics themselves are not secret (and have been confirmed by FBI, regardless of what information NSA provided), it seems possible that the government is being so skittish about these details because they don't actually match what we publicly know. Indeed, at least one detail I've learned about the documents Guccifer 2.0 leaked undermines the neat GRU-FSB narrative.

Comey did confirm something I've been told about the GRU side of the hack: they wanted to be found (whereas the FSB side of the hack had remained undiscovered for months, even in spite of FBI's repeated efforts to warn DNC).

> COMEY: The only thing I'd add is they were unusually loud in their intervention. It's almost as if they didn't care that we knew what they were doing or that they wanted us to see what they were doing. It was very noisy, their intrusions in different institutions.

There is mounting evidence that Guccifer 2.0 went to great lengths to implicate Russia in the

hack. Confirmation GRU also went out of its way to make noise during the DNC hack may suggest both within and outside of the DNC the second hack *wanted* to be discovered.

I have previously pointed to a conflict between what Crowdstrike claimed in its report on the DNC hack and what the FBI told FireEye. Crowdstrike basically said the two hacking groups didn't coordinate at all (which Crowdstrike took as proof of sophistication). Whereas FireEye said they did coordinate (which it took as proof of sophistication and uniqueness of this hack). I understand the truth is closer to the latter. APT 28 largely operated on its own, but at times, when it hit a wall of sorts, it got help from APT 29 (though there may have been some back and forth before APT 29 did share).

All of which brings me to two questions Elise Stefanik asked. First, she asked — casually raising it because it had "been in the news recently" — whether the FSB was collecting intelligence in its hack of Yahoo.

> STEFANIK: Thank you. Taking a further step back of what's been in the news recently, and I'm referring to the Yahoo! hack, the Yahoo! data breech, last week the Department of Justice announced that it was charging hackers with ties to the FSB in the 2014 Yahoo! data breech. Was this hack done to your knowledge for intelligence purposes?
>
> COMEY: I can't say in this forum.
>
> STEFANIK: Press reporting indicates that Yahoo! hacked targeted journalists, dissidence and government officials. Do you know what the FSB did with the information they obtained?
>
> COMEY: Same answer.

Again, in spite of the great deal of detail in the indictment, Comey refused to answer these

obvious questions.

The question is all the more interesting given that the indictment alleges that Alexsey Belan (who was sanctioned along with GRU in December) had access to Yahoo's network until December 2016, well after these hacks. More interestingly, Belan was "minting" Yahoo account credentials at least as late as May 20, 2016. That's significant, because one of the first things that led DNC to be convinced Russia was hacking it was when Ali Chalupa, who was then collecting opposition research on Paul Manafort from anti-Russian entities in Ukraine, kept having her Yahoo account hacked in early May. With the ability to mint cookies, the FSB could have accessed her account without generating a Yahoo notice. Chalupa has recently gone public about some, though not all, of the other frightening things that happened to her last summer (she was sharing them privately at the time). So at a time when the FSB could have accomplished its goals unobtrusively, hackers within the DNC network, Guccifer 2.0 outside of it, and stalkers in the DC area were all alerting Chalupa, at least, to their presence.

While it seems increasingly likely the FSB officers indicted for the Yahoo hack (one of whom has been charged with treason in Russia) were operating at least partly on their own, it's worth noting that overlapping Russian entities had three different ways to access DNC targets.

Note, Dianne Feinstein is the one other person I'm aware of who is fully briefed on the DNC hack and who has mentioned the Yahoo indictment. Like Comey, she was non-committal about whether the Yahoo hack related to the DNC hack.

> Today's charges against hackers and Russian spies for the theft of more than 500 million Yahoo user accounts is the latest evidence of a troubling trend: Russia's sustained use of cyber warfare for both intelligence gathering and financial crimes. The indictment shows

> that Russia used these cyberattacks to target U.S. and Russian government officials, Russian journalists and employees of cybersecurity, financial services and commercial entities.

There seems to be a concerted effort to obscure whether the Yahoo hack had any role in the hack of the DNC or other political targets.

Finally, Stefanik asked Comey a question I had myself.

> STEFANIK: OK, I understand that. How — how did the administration determine who to sanction as part of the election hacking? How — how familiar with that decision process and how is that determination made?
>
> COMEY: I don't know. I'm not familiar with the decision process. The FBI is a factual input but I don't recall and I don't have any personal knowledge of how the decisions are made about who to sanction.

One place you might go to understand the relationship between GRU and FSB would be to Obama's sanctions, which described the intelligence targets this way.

> - *The Main Intelligence Directorate (a.k.a. Glavnoe Razvedyvatel'noe Upravlenie) (a.k.a. GRU) is involved in external collection using human intelligence officers and a variety of technical tools, and is*

> *designated for tampering, altering, or causing a misappropriation of information with the purpose or effect of interfering with the 2016 U.S. election processes.*
>
> - *The Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a FSB) assisted the GRU in conducting the activities described above.*
>
> [snip]
>
> - *Sanctioned individuals include Igor Valentinovich Korobov, the current Chief of the GRU; Sergey Aleksandrovich Gizunov, Deputy Chief of the GRU; Igor Olegovich Kostyukov, a First Deputy Chief of the GRU; and Vladimir Stepanovich Alexseyev, also a First Deputy Chief of the GRU.*

Remember, by the time Obama released these sanctions, several FSB officers, including Dmitry Dokuchaev (who was named in the Yahoo

indictment) had been detained for treason for over three weeks. But the officers named in the sanctions, unlike the private companies and individual hackers, are unlikely to be directly affected by the sanctions.

The sanctions also obscured whether Belan was sanctioned for any role in the DNC hack.

> *Aleksey Alekseyevich Belan engaged in the significant malicious cyber-enabled misappropriation of personal identifiers for private financial gain. Belan compromised the computer networks of at least three major United States-based e-commerce companies.*

Again, all of this suggests that the intelligence community has reason to want to obscure how these various parts fit together, even while publicizing the details of the Yahoo indictment.

Which suggests a big part of the story is about how the public story deviates from the real story the IC is so intent on hiding.