DID GRU LEARN THAT DEMOCRATS HAD HIRED CHRISTOPHER STEELE WHEN THEY HACKED DNC'S EMAIL SERVER?

As I laid out a few weeks ago, I provided information to the FBI on issues related to the Mueller investigation, so I'm going to include disclosure statements on Mueller investigation posts from here on out. I will include the disclosure whether or not the stuff I shared with the FBI pertains to the subject of the post.

According to Glenn Simpson's SJC testimony, he hired Christopher Steele in May or June of 2016 to investigate Trump's ties to Russia.

> Q. And when did you engage Mr. Steele to conduct opposition research on Candidate Trump?
>
> A. I don't specifically recall, but it would 10 have been in the — it would have been May or June of 2016.
>
> Q. And why did you engage Mr. Steele in May or June of 2016?

Simpson is maddeningly vague (undoubtedly deliberately) on this point. In one place he suggests he hired Steele after DCLeaks was registered and amid a bunch of chatter about Democrats being hacked, which would put it after June 8 and probably after June 15.

> Q. So at the time you first hired him had it been publicly reported that there had been a cyber intrusion into the Democratic National Convention computer system?
>
> A. I don't specifically remember. What I

> know was that there was chatter around Washington about hacking of the Democrats and Democratic think tanks and other things like that and there was a site that had sprung up called D.C. Leaks that seemed to suggest that somebody was up to something. I don't think at the time at least that we were particularly focused on — well, I don't specifically remember.

But in his more informative HPSCI testimony, he suggests he may have started talking to Steele about collecting intelligence on Trump in May.

> MR. QUIGLEY: When exactly did he start working under contract?
>
> MR. SIMPSON: My recollection is that, you know, we began talking about the — I don't remember when we started talking about the engagement, but the work started in June, I believe.
>
> MR. QUIGLEY: Okay.
>
> MR. SIMPSON: Possibly late May, but —

Given one detail in Mueller's GRU Indictment, that difference may be critical.

Recall that the DNC figured out they had been hacked in April, and brought in Perkins Coie (the same firm that would engage Fusion GPS) for help. The attorney helping them respond to the hack, Michael Sussmann, warned them not to use DNC email to discuss the hack, because it might alert hackers they were onto them.

> The day before the White House Correspondents' Association dinner in April, Ms. Dacey, the D.N.C.'s chief executive, was preparing for a night of parties when she got an urgent phone call.
>
> With the new monitoring system in place, Mr. Tamene had examined administrative

> logs of the D.N.C.’s computer system and found something very suspicious: An unauthorized person, with administrator-level security status, had gained access to the D.N.C.’s computers.
>
> “Not sure it is related to what the F.B.I. has been noticing,” said one internal D.N.C. email sent on April 29. “The D.N.C. may have been hacked in a serious way this week, with password theft, etc.”
>
> No one knew just how bad the breach was — but it was clear that a lot more than a single filing cabinet worth of materials might have been taken. A secret committee was immediately created, including Ms. Dacey, Ms. Wasserman Schultz, Mr. Brown and Michael Sussmann, a former cybercrimes prosecutor at the Department of Justice who now works at Perkins Coie, the Washington law firm that handles D.N.C. political matters.
>
> “Three most important questions,” Mr. Sussmann wrote to his clients the night the break-in was confirmed. “1) What data was accessed? 2) How was it done? 3) How do we stop it?”
>
> Mr. Sussmann instructed his clients not to use D.N.C. email because they had just one opportunity to lock the hackers out — an effort that could be foiled if the hackers knew that the D.N.C. was on to them.
>
> “You only get one chance to raise the drawbridge,” Mr. Sussmann said. “If the adversaries know you are aware of their presence, they will take steps to burrow in, or erase the logs that show they were present.”
>
> The D.N.C. immediately hired CrowdStrike, a cybersecurity firm, to scan its computers, identify the

> intruders and build a new computer and telephone system from scratch. Within a day, CrowdStrike confirmed that the intrusion had originated in Russia, Mr. Sussmann said.

But it's not clear whether Sussmann warned this small team of people against using DNC emails at all, or just those emails discussing the hack.

Previously, I had always guesstimated how long after DNC brought Crowdstrike in the emails ultimately shared with WikiLeaks got exfiltrated from this analysis, based of the last dates of stolen emails and DNC's email deletion policies in place at the time. It was a damned good estimate — May 19 to May 25.

But according to the indictment, the theft of the DNC emails happened later: starting on May 25, not ending on it.

> Between on or about May 25, 2016 and June 1, 2016, the Conspirators hacked the DNC Microsoft Exchange Server and stole thousands of emails from the work accounts of DNC employees. During that time, YERMAKOV researched PowerShell commands related to accessing and managing the Microsoft Exchange Server.

The indictment doesn't describe the entire universe of emails stolen — whether GRU stole just the 9 email boxes shared with WikiLeaks, or whether they obtained far more.

But the later date — possibly reaching as late as June 1 — means it's possible GRU stole emails involving top DNC officials, officials involved in opposition research activities (as both Guccifer 2.0 and the DNC itself said had been a focus), including the activity of hiring a former MI6 officer to chase down Trump's illicit ties to Russians.

Don't get me wrong. If the Russians did, in fact, learn about the Steele effort and manage

to inject his known reporting chain with disinformation, there were plenty of other possible ways they might have learned of the project: the several people overlapping between Fusion GPS' Prevezon team and its Trump team, Rinat Akhmetshin who learned of the dossier from a chatty NYT editor, or maybe a close Trump ally like Sergei Millian. The sad thing about this disinformation project is it was so widely disseminated, any HUMINT integrity could have easily been compromised early in the process.

But the timeline laid out in the GRU indictment adds one more, even earlier possible way: that Russia learned the Democrats were seeking HUMINT from Russians about Russia's efforts to help Trump from the Democrats' own emails.