BEFORE JOHN DURHAM'S ORIGINATOR-1, THERE WAS A CLAIMED BGP HIJACK

In this post, I described that "Phil," the guy I went to the FBI about because I suspected he had a role in the Guccifer 2.0 persona, had a role in the Alfa Bank story. As noted, Phil's provable role in pushing the Alfa Bank story in October 2016 was minor and would have no effect on the false statement charge — for an alleged lie told in September 2016 — against Michael Sussmann. But because of Durham's sweeping materiality claims, it might have an impact on discovery.

It has to do with the theory that Alfa Bank has about the DNS anomalies, a theory that Durham seems to share: that the data was faked.

As Alfa laid out in its now abandoned John Doe lawsuits, it claims that the anomalous DNS traffic that Michael Sussmann shared with the FBI in September 2016 was faked. The bank appears to believe not just that the data was faked, but that April Lorenzen is involved in some way. For example, it describes that Tea Leaves and "two accomplices" were sources for Franklin Foer (though elsewhere, the lawsuit claims that Tea Leaves was pointed to the data by the unknown John Doe defendants).

Durham seems even more sure that Lorenzen is the culprit. For example, he always refers to the data as "purported." He refers to Lorenzen as "Originator-1" rather than "Data Scientist-1" or "Tea Leaves," insinuating she fabricated the data. And when Sussmann asked for all evidence indicating that Durham had bullied witnesses, Durham provided emails involving Lorenzen's lawyers.

Alfa Bank might be excused for imagining that Lorenzen is the primary culprit to have fabricated the data. According to Krypt3ia, when Alfa asked him for his communications, he only had one email, with a different journalist, to share. They quite clearly don't understand that someone else was involved in publicizing these claims.

Durham doesn't have the same excuse.

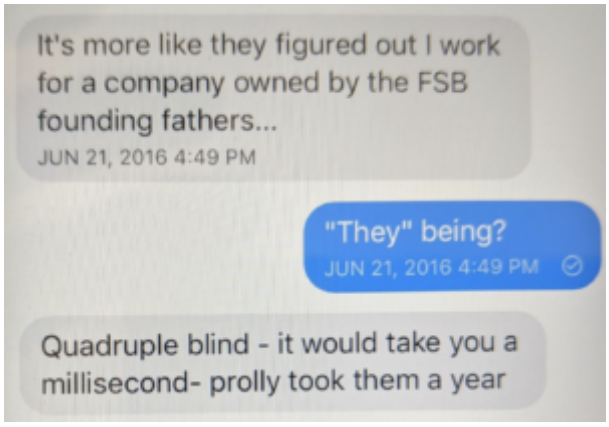
That's because DOJ — of which Durham remains a part — knows at least some of the details about "Phil" that I laid out in my last post. Because they would have checked Twitter to vet some of my most basic claims, they almost certainly obtained the Twitter DMs (or at least the metadata) showing that Phil brokered the tie between Krypt3ia and the NYT.

To be clear: I have no evidence that Phil altered the DNS records. I'm agnostic about what caused the anomaly (though am convinced that the experts involved believe the anomaly is real, even if they offer varying explanations for the cause). But Durham has made the source of the anomaly an issue to bolster his claims about materiality. And, as Sussmann noted in a recent filing, "Much as the Special Counsel may now wish to ignore the allegations in the Indictment, he is bound by them." So, it seems, Durham's on the hook for telling Sussmann if DOJ knows of anyone *else* involved in pushing the Alfa Bank story who could be a possible culprit for fabricating the data, especially if that person was known to have clandestinely signed a comment, "Guccifer 2.0."

Phil probably faked a BGP hijack

The fact that Phil alerted the NYT to the Russian proxy of Lorenzen's data matters not just because he had, months earlier, claimed to work for an FSB-led company and, even before that, claimed to have been coerced by Russian

intelligence at an overseas meeting before the known DNC operation started.



It also matters because (I believe) Phil faked an Internet routing record in the same month the Alfa/Trump/Spectrum anomalies started.

In May 2016, Phil shared what he claimed was a traceroute of a request to my site, an Internet routing record that is different than but related to the DNS records at the heart of the Alfa Bank story. The screencap he sent me purported to show that a request to my site had been routed through (to the best of my memory) some L3 routers in Chicago, to Australia, back to those L3 switches, to my site. Phil was claiming to show me proof that someone had diverted requests to my site overseas along the way — what is known as a BGP hijack. Phil showed this to me in the wake and context of a DDOS attack that had brought my site down for days, an attack which led me to rebuild my site, change hosts, and add Cloudflare DDOS protection.

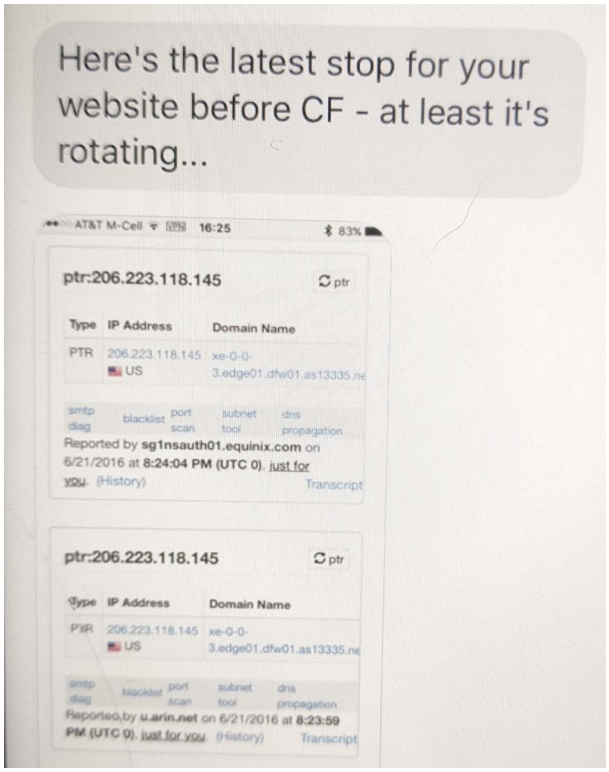
May 2016, the month Phil showed me what I believe to be a faked traceroute, is the same month the anomalous traffic involving Alfa Bank, Spectrum Health, and a Trump-related server started.

Phil used that traceroute to claim that the US intelligence community was diverting and spying on traffic to my website.

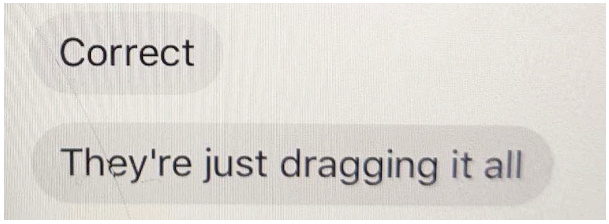
The claim made no sense. The only thing that diverting my traffic would get spies is access

to my readers' metadata, which would be readily accessible via easier means, including with a subpoena to my host provider. Aside from a bunch of drafts that I've decided didn't merit publication, there's no non-public content on my site. I was not competent (and did not ask others) to assess the validity of the screencap itself, but I considered it unreliable because it didn't show the query or originating IP address behind the record, which would be needed to test its provenance.

I don't have that original traceroute (I replaced my phone not long after he sent it). But in June 2016 he shared a reverse DNS look-up related to my site that *wasn't altered* but in which Phil invoked the earlier one.



I corrected him in this case – this IP address was readily explainable; it *was* Cloudflare (which Phil surely knew). But Phil nevertheless repeated his earlier claim that "they" were hijacking my traffic.



When I said that Phil had been tracking how requests to my site worked for some time before he left a comment signed guccifer2.0@kgb.ru in July 2016, this weeks-long exchange is what I was referring to. He had, effectively, been watching as I added Cloudflare protection to my site.

These screencaps show that Phil, who months later would play a role in pushing the Alfa Bank story, was using DNS records — real and possibly faked — as a prop in a false story.

Phil tracked DOD contracts closely

That's not the only detail that DOJ may know about that Durham should consider before insinuating that Lorenzen is the most likely culprit if this data was fabricated. DOJ may know that Phil tracked DOD contracts very closely. That's important because it explains how Phil could have learned researchers would be looking closely at DNS records.

For years, I've believed that the Alfa-Trump-Spectrum Health effort was disinformation, because so much of what came out that year was and because I viewed the Spectrum Health stuff to be such a reach. My belief it might be disinformation only grew stronger when I discovered the focus on Spectrum Health, with its link to Erik Prince's sister's spouse, came just after Prince had asked Roger Stone about his efforts to reach out to WikiLeaks.

Certainly, Putin exploited the allegations afterwards to his advantage. He used them to push Alfa Bank's Petr Aven to take a primary role in reaching out to Trump during the

transition, at least as recounted in the Mueller Report.

> According to Aven, at his Q4 2016 one-on-one meeting with Putin,981 Putin raised the prospect that the United States would impose additional sanctions on Russian interests, including sanctions against Aven and/or Alfa-Bank.982 Putin suggested that Aven needed to take steps to protect himself and Alfa-Bank.983
>
> 981 At the time of his Q4 2016 meeting with Putin, Aven was generally aware of the press coverage about Russian interference in the U.S. election. According to Aven, he did not discuss that topic with Putin at any point, and Putin did not mention the rationale behind the threat of new sanctions

Aven even used Richard Burt, one of the people scrutinized by the Fusion and DNS research, to reach out to Trump, effectively pursuing precisely the back channel between Alfa and Trump that Fusion suspected months earlier.

The relevant part of Aven's interview is redacted, so it's not clear whether Aven mentioned that Alfa Bank had been a key focus of the interference allegations. But that's the presumptive subtext: along with the Steele dossier, the DNS anomaly — both of which, in several lawsuits since, Aven or Alfa have claimed were "gravely damaging" — raised suspicions about Alfa Bank and made it more likely the bank would be sanctioned than had been the case previously.

And before the bank *did* get sanctioned last month, Alfa was using the DNS anomaly to conduct a lawfare campaign to learn how the US uses DNS tracking to thwart hacks (one wonders if Putin ordered that campaign, like he personally ordered Aven to reach out to Trump). That campaign even got a bunch of frothy right-

wingers to decry efforts to prevent and detect nation-state hacks on the US. So at the very least, Russia has exploited the Alfa-Trump allegations to great benefit, one measure of whether something could be deliberate disinformation.

But as I've talked to people who've tried to figure out what the anomaly was — including experts who believed it did reflect real communication as well as some who didn't — they always explained that seeding disinformation in such a fashion would be useless. That's because you couldn't ensure that any disinformation you planted would be seen. That is, unlike the Steele dossier, which was being collected by an Oleg Deripaska associate and shared with the press (and for which there's far more evidence Russia used it to plant disinformation), you could never expect the disinformation to be noisy enough to attract the desired attention.

In the years since the original story, how researchers who found the anomalous data obtained the DNS data has driven a lot of the hostility behind it. The researchers have tried to hide where they got the data for proprietary and cybersecurity reasons. John Durham has alleged there was some legal impropriety behind using it, even when used (as the researchers understood they were doing) to research ongoing nation-state hacks. And Alfa Bank was using lawfare to try to find out as much about the means by which this DNS traffic was observed by cybersecurity experts as possible. The full story of how the researchers accessed the data has yet to be reported, but as I understand it, there's more complexity to the question than initially made out or than has made it into Durham's court filings. That complexity would make it even harder to anticipate where DNS researchers were looking. So, multiple experts told me, it would be crazy to imagine anyone would have thought to seed disinformation in DNS records expecting it'd get picked up via those collection points in 2016, because no one would have expected anyone was observing all those

collection points.

If a Fancy Bear shits in the DNS woods but there's no one there to see it, did it really happen?

But there was, in fact, a way to anticipate it might get seen.

As the Sussmann indictment vaguely alluded to and this NYT story laid out in detail, researchers found the DNS anomalies in the context of preparing a bid for a DARPA research contract.

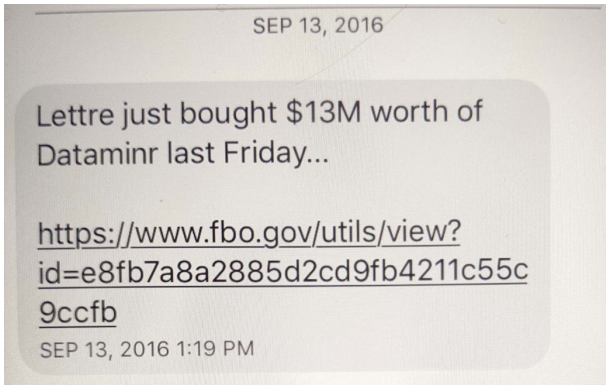
> The involvement of the researchers traces back to the spring of 2016. DARPA, the Pentagon's research funding agency, wanted to commission data scientists to develop the use of so-called DNS logs, records of when servers have prepared to communicate with other servers over the internet, as a tool for hacking investigations.
>
> DARPA identified Georgia Tech as a potential recipient of funding and encouraged researchers there to develop examples. Mr. Antonakakis and Mr. Dagon reached out to Mr. Joffe to gain access to Neustar's repository of DNS logs, people familiar with the matter said, and began sifting them.
>
> Separately, when the news broke in June 2016 that Russia had hacked the Democratic National Committee's servers, Mr. Dagon and Ms. Lorenzen began talking at a conference about whether such data might uncover other election-related hacking.

The DOD bidding process provided public notice that DARPA was asking researchers to explore multiple ways, including DNS traffic, to attribute persistent hacking campaigns in real time.

The initial DARPA RFP was posted on April 22,

2016, ten days before the anomalous traffic started but well after the Russian hacking campaign had launched (documents FOIAed by the frothers reveal that the project was under discussion for months before that). This RFP provided a way for anyone who tracked DOD contracts closely to know that people would be looking and the announcement itself included DNS records and network infrastructure among its desired measurements. Depending on the means by which DARPA communicated about the contract, it might also provide a way to find out *who* would be looking and *how* and *where* they would be looking, though as I understand it, the team at Georgia Tech would have been an obvious choice in any case.

Phil tracked DOD contracts very closely. In September 2016, for example, he sent me a text alerting me to a new Dataminr contract just 66 minutes after I published a post about the company (I later wrote up the contract).



Phil also told me, verbally, he was checking what contracts DOD had with one of the US tech companies for which a back door was exposed in summer 2016. He claimed he was doing so to see how badly the government had fucked itself with its failure to disclose the vulnerability. By memory (though I am not certain), I believe it was Juniper Networks, in the wake of the Shadow Brokers release of an NSA exploit targeting the company.

And even on top of Phil's efforts to convince me that the DNC hack wasn't done by APT 28, DOJ has other evidence that Phil tracked APT attribution

efforts closely, even using official government resources to do so. So it would be unsurprising if he had taken an interest in a contract on APT attribution in real time.

Durham may have access to some or all of this

Durham insinuates the DNS records are faked and he appears to want to blame Lorenzen for faking them. But he may be ignoring evidence in DOJ's possession that someone else who, I've now confirmed, played at least a minor role in pushing the Alfa Bank story was using Internet routing records, possibly faked, to support a false story in May 2016.

To be sure: while I know the investigation into Phil continued at least the better part of a year after my FBI interview about him, any feedback I've gotten about that investigation has been deliberately vague. So aside from the obvious things — like the Twitter records that would show Phil's DMs with Krypt3ia and Nicole Perloth — I can't be sure what is in DOJ's possession.

I don't even know whether the 302 from my FBI interview would mention Phil's pitch of the Alfa Bank story to me. It was on a list of the things I had intended to describe in that interview. But I didn't work from the list in the interview itself and I have no affirmative memory of having mentioned it. If I did, it would have amounted to me saying little more than, "he also was pushing the Alfa Bank story."

That said, unless the FBI agents were epically incompetent, my 302 should mention Alfa Bank, because I'm absolutely certain I raised this post and its emphasis on the inclusion of Alfa Bank in an alarming April 2017 BGP hijack.

And in fact, there's a way Durham could have found out about Phil's role in the Alfa Bank story independent of my FBI interview. Of just two people in the US government with whom I

shared some of the Alfa Bank-related texts I exchanged with Phil (both were Republicans), one was centrally involved in the investigations that fed into the Durham investigation. If this stuff matters, Durham should ask why several of his key source investigations didn't focus on it.

Durham *should* know that Phil had a role in the Alfa Bank story.

And given his insinuations in the indictment that Lorenzen fabricated DNS data in May 2016, making the insinuation part of his materiality claims, Durham may be obligated to tell Michael Sussmann that DOJ already knows of someone who was pushing the Alfa Bank story who used DNS data to tell a false story in May and June 2016.