JOHN DURHAM'S TOP PROSECUTOR, ANDREW DEFILIPPIS, ALLEGEDLY MIFFED THAT DARPA INVESTIGATED GUCCIFER 2.0

Vladimir Putin's invasion of Ukraine and the sanctions imposed as a result has led lawyers in the US to drop the now-sanctioned Alfa Bank and its owners, leading to the dismissal of the John Doe, BuzzFeed, and Fusion GPS lawsuits filed by Alfa Bank or its owners. That has, for now, brought an end to a sustained Russian effort to use lawfare to discover "U.S. cybersecurity methods and means" (as some of Alfa's targets described the effort).

But the dismissal of the Alfa Bank suits hasn't halted the effort to expose US cybersecurity efforts in the guise of pursuing right wing conspiracy theories. Both Federalist Faceplant Margot Cleveland and "online sleuths" goaded, in part, by Sergei Millian have picked up where Alfa Bank left off. In recent days, for example, documents obtained via a Federalist FOIA to Georgia Tech exposed the members of a cybersecurity sharing group, including a bunch at Three-Letter Agencies, which has little news value but plenty of intelligence value to America's adversaries (these names were released even while someone — either Georgia Tech or the Federalist — chose to redact the contact information for Durham's investigators, some of which is otherwise public).

Even while doing her part to make America less safe (raising the perennial question of who funds the Federalist), Cleveland has continued to do astounding work misrepresenting Durham's investigation. From the same FOIA release, she published a document in which research scientist

Manos Antonakakis described that chief Durham AUSA Andrew DeFilippis insinuated to him that it was abusive for DARPA to try to discover the network behind the Guccifer 2.0 persona.

> Finally, I will leave you with an anecdote and a thought. During one of my interviews with the Special Counsel prosecutor, I was asked point blank by Mr. DeFilippis, "Do you believe that DARPA should be instructing you to investigate the origins of a hacker (Guccifer_2.0) that hacked a political entity (DNC)?" Let that sync for a moment, folks. Someone hacked a political party (DNC, in this case), in the middle of an election year (2016), and the lead investigator of DoJ's special council would question whether US researchers working for DARPA should conduct investigations in this matter is "acceptable"! While I was tempted to say back to him "What if this hacker hacked GOP? Would you want me to investigate him then?", I kept my cool and I told him that this is a question for DARPA's director, and not for me to answer.

Assuming this is an accurate description, this is a shocking anecdote, a betrayal of US national security.

It suggests that Durham's lead prosecutor doesn't believe the government should throw its most innovative research at a hostile nation-state attack *while* that nation-state is attempting to influence an election. Sadly, though, it's not surprising.

It is consistent with things we've seen from Durham's team throughout. It's consistent with Durham's treatment of a loose tie between an indirect and unwitting Steele dossier source and the Hillary campaign as a bigger threat than multiple ties to Russian intelligence (or Dmitry Peskov's office, which knew that Michael Cohen and Donald Trump were lying about the former's

secret communications with Peskov's office). It is consistent with Durham's more recent suggestion that the victim of such a nation-state attack must wait until after an election to report a tip that might implicate her opponent.

I almost feel like DeFilippis will eventually say Hillary should have just laid back and enjoyed being hacked in 2016.

DeFilippis, and Durham generally, have consistently treated Hillary as a far graver threat than Russia, even now, even as Russia conducts a barbaric invasion of a peaceful democracy.

But Antonakakis' anecdote is all the more troubling because it suggests that DeFilippis seems to misunderstand what happened with the DARPA contract in question in 2016. The Enhanced Attribution RFP's description of the hacking campaigns it was targeting — "multiple concurrent independent malicious cyber campaigns, each involving several operators" — pretty obviously aims to tackle Advanced Persistent Threats, of which APT 28 and 29 (both of which targeted the DNC) were among the most pressing in 2016. DARPA presumably didn't ask Antonakakis to focus on Guccifer 2.0 — a persona which didn't exist when the contract was put up for bid in April 2016, much less in the months earlier when it was originally conceived. Rather, by description, they were asking bidders to look at APTs, and looking at APT 28 would have happened to include looking at Guccifer 2.0, the DNC hack, and a number of hacks elsewhere in the US and the world. The reason DARPA would ask Georgia Tech to look at APT 28 is because APT 28 was hacking a lot of targets in the time period, all of which provided learning sets for a researcher like Antonakakis. DeFilippis, then, seems miffed that the APT that DARPA wanted to combat happened to be one of two that targeted Hillary.

That's a choice Russia made, not DARPA.

While I think Cleveland did serious damage with some of her releases, I'm glad she released *this* document because it provides a way for Michael Sussmann to make DeFilippis' troubling views on national security a central issue at trial, something that normally is difficult to do.

It also provided Cleveland another opportunity to faceplant in spectacular trademark Federalist fashion. Cleveland used this document to rile up the frothers by suggesting this is proof that Durham is investigating the DNC attribution.

> ## *Exclusive: Special Counsel's Office Is Investigating The 2016 DNC Server Hack*
>
> The U.S. Department of Defense tasked the same Georgia Tech researcher embroiled in the Alfa Bank hoax with investigating the "origins" of the Democratic National Committee hacker, according to an email first obtained by The Federalist on Wednesday. That email also indicates the special counsel's office is investigating the investigation into the DNC hack and that prosecutors harbor concerns about the DOD's decision to involve the Georgia Tech researcher in its probe.
>
> [snip]
>
> The public storyline until now had been that CrowdStrike, the cybersecurity firm Sussmann hired in April 2016, had concluded Russians had hacked the DNC server, and that the FBI, which never examined the server, concurred in that conclusion. Intelligence agencies and former Special Counsel Robert Mueller likewise concluded that Russian agents were behind the DNC hack, but with little public details provided.

> It now appears that DARPA had some role in that assessment, or rather Antonakakis did on behalf of DARPA, which leads to a whole host of other questions, including whether DARPA had access to the DNC server and data and, if so, from whom did the DOD's research arm get that access? Was it Sussmann?

There's no reason to believe this and every reason to believe that — as I said — DeFilippis is pissed that DARPA prioritized their research on a target that was badly affecting national security (and not just in US, but also in allied countries) in 2016, one that happened to attempt to help Trump get elected.

But look how many errors Faceplant's Cleveland made in the process:

Cleveland repeats the Single Server Fallacy, imagining that the DNC, DCCC, and Hillary had just one server between them to be hacked and all the servers that got hacked were in the possession of one of those victims. That's, of course, ridiculous. The server that GRU hacked to get John Podesta's emails belonged to Google. The server that GRU hacked to get Hillary's analytics belonged to AWS. There was a staging server in AZ; I have been told that the FBI seized at least one US-based server that did not belong to the DNC (that server is why the frothy right's focus on what Shawn Henry testified to HPSCI is so painfully ignorant — because it ignores that the FBI had access to servers that Henry did not that *did* show exfiltration).

Cleveland apparently doesn't know that FBI knew who was hacking the DNC when they warned them starting in September 2015 they were being hacked. The FBI's awareness of that not only explains why APT 29 and 28 would have been included in DARPA's targets for EA, but proves that the government was tracking these hacking groups above and beyond the attack on Hillary. This was never just a reaction to the election year hack.

Cleveland claims Mueller's attribution of the DNC hack to the GRU provided "little public details," when in fact the Mueller Report showed 29 sources other than CrowdStrike, including:

- Gmail
- Linked-In
- Microsoft
- Facebook
- Twitter
- WordPress
- ActBlue
- AWS
- AOL
- Smartech Corporation
- URL shortening service
- Bitcoin exchanges
- VPN services

According to Mueller's report, all these sources also corroborated the GRU attribution. And Mueller's list doesn't include a number of other known entities that corroborated the attribution, including NSA and Dutch intelligence, which couldn't be named in a public DOJ document. Mueller's list doesn't include Georgia Tech either, but it wouldn't need to, because there was so much other evidence.

The Mueller Report described obtaining almost 500 warrants, but the released list — from which FBI's Cyber Division successfully withheld those pertaining to the GRU investigation — only includes around 370-400 warrants (based on an 156 pages of warrants with roughly three per page), suggesting there may be 100 warrants tied to the GRU attribution alone.

By the time Antonakakis started looking at the DNC hack as part of EA, multiple entities, including several Infosec contractors, non-US intelligence services, and non-governmental entities like tech giants (including at least

three of the ones on Mueller's list), had plenty of evidence that the Guccifer 2.0 campaign was run by the APT 28. Including Guccifer 2.0 as part of the research set would simply be part of the existing targeting of a dangerous APT.

But apparently neither DeFilippis nor Cleveland understand that 2016 was part of an ongoing identified threat to US national security.

One thing Putin did in 2016 was to use disinformation to train the frothy right to favor Russia more than fellow Americans from the opposing party. Even as Russia attacks Ukraine, that still seems to be true.