IN INDICTMENT ACCUSING MICHAEL SUSSMANN OF HIDING DETAILS ABOUT RESEARCHERS, JOHN DURHAM HID DETAILS ABOUT RESEARCHERS

In my initial John Durham Is the Jim Jordan of Ken Starrs post pointing to all the problems with John Durham's attempt to criminalize victims reporting on information operations, I described Durham's description of why Michael Sussmann's alleged lie was material.

> SUSSMANN's lie was material because, among other reasons, SUSSMANN's false statement misled the FBI General Counsel and other FBI personnel concerning the political nature of his work and deprived the FBI of information that might have permitted it more fully to assess and uncover the origins of the relevant data and technical analysis, including the identities and motivations of SUSSMANN's clients.
>
> Had the FBI uncovered the origins of the relevant data and analysis and as alleged below, it might have learned, among other things that (i) in compiling and analyzing the Russian Bank-1 allegations, Tech Executive-1 had exploited his access to non-public data at multiple Internet companies to conduct opposition research concerning Trump; (ii) **in furtherance of these efforts, Tech Executive-1 had enlisted, and was continuing to enlist, the assistance of researchers at a U.S.-based university who were receiving and**

> **analyzing Internet data in connection with a pending federal government cybersecurity research contract**; and (iii) SUSSMAN, Tech Executive-1, and Law Firm-1 had coordinated, and were continuing to coordinate, with representatives and agents of the Clinton Campaign with regard to the data and written materials that Sussmann gave to the FBI and the media. [my emphasis]

John Durham says it is a crime to hide details about the researchers who first identified the Alfa Bank anomaly.

Yet, even based on the indictment, I identified a number of holes in Durham's description of what the researchers had done. Yesterday, NYT and CNN both published stories identifying the four researchers — Rodney Joffe (Tech Executive-1), April Lorenzen (Tea Leaves, whom Durham needlessly renamed Originator-1), Manos Antonakakis (Researcher-1), and David Dagon (Researcher-2) — showing that the holes I identified in the indictment indeed left out information that totally undermined Durham's insinuations.

For example, I noted that the date when what NYT identifies as DARPA shared information with the researchers is important to identify whether they obtained the data in order to research Trump.

> At some point [Durham doesn't provide even a month, but by context it was at least as early as July 2016 and could have been far, far earlier], TE-1's company provided a university with data for a government contract ultimately not contracted until November 2016, including the DNS data from an Executive Branch office of the US government that Tech Exec-1's company had gotten as a sub-contractor to the US government. [This date of this is critical because it would be the trigger for a Conspiracy

> to Defraud charge, if Durham goes there.]

NYT describes that DARPA first approached potential partners in the spring, long before Sussman or Joffe got involved.

> 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.

I noted that Durham didn't give the date when Lorenzen first started looking at the the DNS data. That date is another read of whether she had done so out of malice targeting Trump.

> By some time in late July 2016 [the exact date Durham doesn't provide], a guy who always operated under the pseudonym Tea Leaves but whom Durham heavy-handedly calls "Originator-1" instead had assembled "purported DNS data" reflecting apparent DNS lookups between Alfa Bank and "mail1.trump-email.com" that spanned from May 4 through July 29.

NYT reveals that Lorenzen and Dagon first started talking about using the DNS data to check other election-related hacking at a conference that went from June 13 to June 16

(meaning, the DNC hack would have been revealed during the conference).

> 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.
>
> Ms. Lorenzen eventually noticed an odd pattern: a server called mail1.trump-email.com appeared to be communicating almost exclusively with servers at Alfa Bank and Spectrum Health. She shared her findings with Mr. Dagon, the people said, and they both discussed it with Mr. Joffe.

I noted that Durham had left out all mention of the WikiLeaks release and Trump's invitation to Russia to keep hacking his opponent.

> It appears (though Durham obscures this point) that all the actions laid out in this indictment post-date the press conference. Virtually everyone in the US committed to ensuring America's national security was alarmed by Trump's comments in this press conference. Yet Durham doesn't acknowledge that all these actions took place in the wake of public comments that made it reasonable for those committed to cybersecurity to treat Donald Trump as a national security threat, irrespective of partisan affiliation.
>
> Durham will work hard to exclude detail of Trump's press conference from trial. But I assume that if any of the named subjects of this investigation were to take the stand at trial, they would point out that it was objectively reasonable after July 27 to have national security concerns based on

> Trump's encouragement of Russia's attack on Hillary Clinton and his defensive denials of any business ties. Any of the named subjects of the indictment would be able to make a strong case that there was reason to want to, as a matter of national security, test Trump's claim to have no financial ties to Russia. Indeed, the bipartisan SSCI Report concluded that Trump posed multiple counterintelligence concerns, and therefore has concluded that Durham's portrayal of politics as the only potential motive here to be false.
>
> Central to Durham's theory of prosecution is that there was no sound national security basis to respond to anomalous forensic data suggesting a possible financial tie between Trump and Russia. Except that, after that July 27 speech — and all of these events appear to post-date it — that theory is unsustainable.

NYT reveals that when Dagon shared the data with Joffe on July 29, he did so in the context of those two events.

> "Half the time I stop myself and wonder: am I really seeing evidence of espionage on behalf of a presidential candidate?" Mr. Dagon wrote in an email to Mr. Joffe on July 29, after WikiLeaks made public stolen Democratic emails timed to disrupt the party's convention and Mr. Trump urged Russia to hack Mrs. Clinton.

I noted that Durham was probably wrong to believe that an August discussion about whether the data could have been spoofed was inculpatory.

> Still others (such as the recognition that this could be spoofed data) will almost certainly end up being presented

> as exculpatory if this ever goes to trial, but Durham seems to think is inculpatory.

NYT describes that a later discussion doubted that the data could have been spoofed.

> The indictment quotes August emails from Ms. Lorenzen and Mr. Antonakakis worrying that they might not know if someone had faked the DNS data. But people familiar with the matter said the indictment omitted later discussion of reasons to doubt any attempt to spoof the overall pattern could go undetected.

I noted that Durham attributed the view that the DNS traffic was a "red herring" to everyone involved, including Sussmann, even though Sussmann appears not to have been on the email.

> In one place, Durham describes "aforementioned views," plural, that the Alfa Bank data was a "red herring," something only attributed to TE-1 in the indictment, seemingly presenting TE-1's stated view on August 21 to everyone involved, including Sussmann, who does not appear to have been on that email chain.

NYT describes that after that, Joffe came to discount the marketing server explanation.

> Mr. Tyrrell, his lawyer, said that research in the weeks that followed, omitted by the indictment, had yielded evidence that the specific subsidiary server in apparent contact with Alfa Bank had not been used to send bulk marketing emails. That further discussion, he said, changed his client's mind about whether it was a red herring.
>
> "The quotation of the 'red herring'

> email is deeply misleading," he said, adding: "The research process is iterative and this is exactly how it should work. Their efforts culminated in the well-supported conclusions that were ultimately delivered to the F.B.I."

It also explains that in context, Joffe referenced a June article describing Trump's interest in a Trump Tower Moscow.

> The indictment says Mr. Joffe sent an email on Aug. 21 urging more research about Mr. Trump, which he stated could "give the base of a very useful narrative," while also expressing a belief that the Trump server at issue was "a red herring" and they should ignore it because it had been used by the mass-marketing company.
>
> The full email provides context: Mr. Trump had claimed he had no dealings in Russia and yet many links appeared to exist, Mr. Joffe noted, citing an article that discussed aspirations to build a Trump Tower in Moscow. Despite the "red herring" line, the same email also showed that Mr. Joffe nevertheless remained suspicious about Alfa Bank, proposing a deeper hunt in the data "for the anomalies that we believe exist."
>
> He wrote: "If we can show possible email communication between" any Trump server and an Alfa Bank server "that has occurred in the last few weeks, we have the beginning of a narrative," adding that such communications with any "Russian or Ukrainian financial institutions would give the base of a very useful narrative."

In my post, I noted that Durham neglected to describe that the researchers turned out to correctly suspect Trump was hiding efforts to

broker a Trump Tower deal.

> According to Michael Cohen, when Trump walked off the stage from that July 27 press conference, Cohen asked Trump why he had claimed that he had zero business ties with Russia when he had in fact been pursuing an impossibly lucrative deal to brand a Trump Tower in Moscow. And we now know that within hours of Trump's request, GRU hackers made a renewed assault on Hillary's own servers. By the time security researchers pursued anomalous data suggesting covert communications with a Russian bank, Cohen had already participated in discussions about working with two sanctioned Russian banks to fund the Trump Tower deal, had agreed to work with a former GRU officer to broker it, had spoken to an aide of Dmitry Peskov, and had been told that Putin was personally involved in making the deal happen. Just on the Trump Tower basis alone, Trump had publicly lied in such a way that posed a counterintelligence risk to America.

In my post, I noted that Durham downplayed that, when Joffe asked the researchers if the paper Sussmann wrote was plausible, they said it was.

> On September 14, TE-1 [not Sussmann] sent the white paper he had drafted to Researcher 1, Researcher 2, and Tea Leaves to ask them if a review of less than an hour would show this to be plausible. Though some of them noted how limited the standard of "plausibility" was, they agreed it was plausible, and Researcher 2 said [Durham does not quote the specific language here] "the paper should be shared with government officials."

NYT describes that Durham misrepresented the

enthusiasm with which Lorenzen "wholeheartedly" expressed her belief the explanation was plausible.

> The indictment also quoted from emails in mid-September, when the researchers were discussing a paper on their suspicions that Mr. Sussmann would soon take to the F.B.I. It says Mr. Joffe asked if the paper's hypothesis would strike security experts as a "plausible explanation."
>
> The paper's conclusion was somewhat qualified, an email shows, saying "there were other possible explanations," but the only "plausible" one was that Alfa Bank and the Trump Organization had taken steps "to obfuscate their communications."
>
> The indictment suggested Ms. Lorenzen's reaction to the paper was guarded, describing an email from her as "stating, in part, that it was 'plausible' in the 'narrow scope' defined by" Mr. Joffe. But the text of her email displays enthusiasm.
>
> "In the narrow scope of what you have defined above, I agree wholeheartedly that it is plausible," she wrote, adding: "If the white paper intends to say that there are communications between at least Alfa and Trump, which are being intentionally hidden by Alfa and Trump I absolutely believe that is the case," her email said.

NYT shows several more ways that Durham utterly misrepresented how seriously the researchers took this thesis.

> The indictment cited emails by Mr. Antonakakis in August in which he flagged holes and noted they disliked Mr. Trump, and in September in which he approvingly noted that the paper did not

> get into a technical issue that specialists would raise.
>
> Mr. Antonakakis' lawyer, Mark E. Schamel, said his client had provided "feedback on an early draft of data that was cause for additional investigation." And, he said, their hypothesis "to this day, remains a plausible working theory."
>
> The indictment also suggests Mr. Dagon's support for the paper's hypothesis was qualified, describing his email response as "acknowledging that questions remained, but stating, in substance and in part, that the paper should be shared with government officials."
>
> The text of that email shows Mr. Dagon was forcefully supportive. He proposed editing the paper to declare as "fact" that it was clear "that there are hidden communications between Trump and Alfa Bank," and said he believed the findings met the probable cause standard to open a criminal investigation.
>
> "Hopefully the intended audience are officials with subpoena powers, who can investigate the purpose" of the apparent Alfa Bank connection, Mr. Dagon wrote.

One of the first things Michael Sussmann is going to do after this story is request information on what the grand jury was told, including whether any of this was affirmatively misrepresented to the grand jury.

The sheer amount of communications that, in days, these researchers have been able to prove were misrepresented, too, suggests DOJ has cause to review whether Durham misrepresented the substance of this indictment to those who approved it, up to and including Merrick Garland.

John Durham says it is a crime to lie about

these researchers in an effort to launch an investigation. And yet, the available evidence suggests he did just that.

Update: To be clear, he can’t be prosecuted for any of this. Prosecutors have expansive immunity for such things.