JOHN DURHAM IS THE JIM JORDAN OF KEN STARRS

Last Thursday, John Durham indicted Michael Sussmann, the Perkins Coie lawyer who advised the DNC, DCCC, and Clinton Campaign about cybersecurity in 2016 as they struggled to deal with a hostile nation-state attack aiming — in part — to help elect their opponent. The indictment accuses Sussmann of lying to FBI General Counsel James Baker at a September 19, 2016 meeting at which Sussmann shared information about the curious DNS traffic between a server used by a Trump marketing contractor and Alfa Bank.

emptywheel's long history of debunking the Alfa Bank story

Before I unpack the indictment, let me remind readers that when this story first publicly broke, I explained why the Spectrum Health (aka my boob hospital at the time) aspect of the allegations made no sense, criticized Hillary's team (including Jake Sullivan) for jumping on the story, and echoed Rob Graham's criticism of the researchers who accessed DNS data to conduct this research.

> In addition to his technical debunking, Robert Graham made an equally important point: researchers shouldn't be accessing this data for ad-lib investigations into presidential candidates, and it's not even clear who would have access to it all except the NSA.
>
> > The big story isn't the conspiracy theory about Trump, but that these malware

> > researchers exploited their privileged access for some purpose other than malware research.
> >
> > [snip]
> >
> > In short, of all the sources of "DNS malware information" I've heard about, none of it would deliver the information these researchers claim to have (well, except the NSA with their transatlantic undersea taps, of course).
>
> [snip]
>
> [B]efore Tea Leaves started pushing this story to the press, the FBI had been investigating it for two months.
>
> Which, to my mind, raises even more questions about the anonymous researchers' identities, because (small world and all) the FBI likely knows them, in which case they may have known that the FBI wasn't jumping on the story by the time they started pitching it.
>
> Or the FBI doesn't know them, which raises still more questions about the provenance of these files.
>
> Ah well, if President Hillary starts a war with Russia based off Iraq-War style dodgy documents, at least I'll have the satisfaction of knowing my boob clinic is right there on the front lines.

In March 2017, I observed that the weird Alfa Bank entry in the Steele dossier suggested a feedback loop between the Alfa Bank server story and the dossier project. Then days after that, I noted all the ways that the packaging of this story made it more suspect.

In 2018, I complained about the way Dexter

Filkins had strained to sustain the story, while noting that people ought to look more closely at why Alfa Bank might be the focus here; the Mueller Report since confirmed that within weeks after the story broke publicly, Vladimir Putin pushed Oligarchs from Alfa Bank to fight harder against western sanctions, something that the alleged source for the Alfa Bank entry in the dossier seemed to parrot.

In short, I not only have consistently criticized this story, but done so in ways that anticipate the most justifiable parts of the indictment. It's only the last bit — how the Alfa narrative echoes Putin's interests — that this indictment doesn't incorporate.

I guess with five more years Durham might get there…

So in unpacking this indictment, I'm in no way defending the Alfa Bank — Trump Tower story. It was a sketchy allegation, the packaging of it was suspect, and those who conducted the research arguably violated ethical guidelines.

I got to where Durham got in this indictment years and years ago. But that doesn't make it a crime.

John Durham's "narrative"

Moreover, that doesn't mean Durham should tell as strained a "narrative" as those who packaged up this story. Central to Durham's indictment is an assumption that if a victim of a crime who believed at the time that the crime had a — since confirmed — political goal reports suspicious, potentially related details, the victim must be motivated exclusively out of self-interest, not good citizenship or a concern about national security. That is, this entire indictment assumes that when Russia attacks a Presidential candidate, that is not itself a national security concern, but instead nothing more than a political dispute.

Effectively, John Durham has made it a crime for someone victimized by a Russian influence operation to try to chase down Russian influence operations.

Tech Executive-1 and Clinton both had retained Perkins Coie long before this, with Sussmann getting involved specifically for cybersecurity help in the wake of the Russian hack

The indictment, perhaps deliberately, obscures the timeline and facts leading up to the charged lie. But here's the story it tells. First, all of Durham's subjects established contracts with each other, even though all of those contracts (including Fusion GPS') had scopes far larger than oppo research on Trump's relationship with Russia.

- In February 2015, Tech Executive-1 (whom I'll call TE-1 for brevity) retained Sussmann to deal with a US government agency [Durham does not say whether this matter was resolved or continued in this period in 2016, which is central to the question of what kind of client of Sussmann's TE-1 was].
- In April 2015, the Clinton Campaign retained Perkins Coie and made Marc Elias the Campaign's General Counsel.
- In April 2016, the victim of a Russian government

election-related attack, the DNC, retained Sussmann to help it deal with aftermath, which included meeting with the FBI. As the indictment describes this was not just legal support but cybersecurity.

- [After a Republican retained them first and on a date that Durham doesn't reveal,] Perkins Coie retained Fusion GPS to conduct oppo research on Trump pertaining to Russia [and other topics, though Durham doesn't mention those other topics].

Durham only mentions in passing, later, that the researchers involved here similarly knew each other through relationships that focused on cybersecurity and predated these events.

Via means and on specific dates that Durham doesn't always provide, Tea Leaves, TE-1, Sussmann, and two Researchers got the DNS data showing an anomaly

There are two sets of research here: that done in a university setting and that done at companies associated with TE-1, though TE-1 is the pivot to both. As depicted, Durham suggests the former are more legally exposed than the latter.

- 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.

- Tea Leaves was a business associate of TE-1 and via means Durham doesn’t describe, the data Tea Leaves gathered was shared with TE-1.
- “In or about July 2016” [at a time that, because of the laws of physics, must post-date the late July date when Tea Leaves collected this data and the date when he shared them with TE-1], TE-1 alerted Sussmann to the data.
- On July 31, Sussmann billed the Clinton Campaign for 24 minutes with the billing description, “communications with Marc Elias regarding server issue.”
- 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.]

- In or about August 2016 [Durham doesn't provide a date], a federal government was finalizing but had not yet signed a cybersecurity research contract with [presumably] that same university to receive and analyze large quantities of public and non-public data "to identify the perpetrators of malicious cyber-attacks and protect U.S. national security." Tea Leaves was the founder of a company that the university was considering [Durham doesn't provide the date of consideration, but generally these things precede finalization] for a

subcontract with the government contract.

TE-1 directs employees of companies under his control to research this issue

Though Durham's indictment is somewhat vague, at least one piece of research from companies associated with TE-1 was shared with the FBI; it appears that other threads of research were not shared.

- In or about early August 2016 [the dates of which Durham doesn't provide], TE-1 directed personnel at two companies in which he had an ownership interest to search for what the indictment calls, "any Internet data reflecting potential connections or communications between Trump or his associates and Russia," which Durham describes to be "derogatory information on Trump." In connection with this tasking, TE-1 later stated [on a date Durham doesn't describe] he was working with someone who had close ties to the Democratic Party.
- At some point, an individual tasked with this work described being "uncomfortable regarding

this tasking," [Durham doesn't describe when he learned this or whether there is any contemporaneous proof].

- At some point [Durham doesn't describe the date], TE-1 provided one of his companies with personal (but publicly available) data from six Trump associates and one purported US-based lobbyist for Alfa Bank and directed these individuals should be the focus of that company's data queries and analysis [Durham doesn't say whether these six associates overlapped with the people Fusion had been tasked to research, nor does he allege they got included in the eventual reports to the FBI; both details are needed to assess his case].
- On August 12, 2016, Sussmann, Elias, and TE-1 met in Elias' office; Sussmann billed his time to the Clinton Campaign describing, "confidential meetings with Elias, others."
- On August 15, employees at one of the companies queried their holdings against a set of addresses that referred

to Trump and/or Alfa Bank.

- During the same time period [Durham doesn't specify when], employees at Internet Company-3 drafted a written paper that included technical observations that Sussmann would later convey to the FBI.

Around the time this started, Sussmann met Fusion and a bunch of meetings happened that were billed to Hillary

- On July 29, Sussmann and Marc Elias met with Fusion GPS [Durham doesn't affirmatively claim this data pertained to the server issue], and Sussmann billed his time to the Hillary Campaign under "General Political Advice," a different description than all the other Fusion meetings that Durham more credibly claims relate to the Alfa Bank allegation.
- Around "the same [August] time period" [Durham doesn't provide the date], Sussmann, Elias, and Fusion personnel began exchanging emails with the subject line, "Connecting you all by

email;" [Durham doesn't say who initiated the email, but it suggests that before this period, Sussmann and Fusion did not have direct contact].

- On August 17, 2016, Sussmann, Elias, and TE-1 conducted an additional conference call, for which Sussmann billed his time to the Clinton campaign, noting "telephone conference with" TE-1 and Elias.
- On August 19, 2016, Sussman and Elias had another in-person meeting that Sussmann described as a meeting with TE-1, which was billed as a "confidential meeting with Elias, others."

Researchers 1 and 2 and Tea Leaves worked with TE-1 on a "storyline" and "narrative" with varying degrees of skepticism expressed

This is the stuff Durham—with some justification—will and has used to taint all this as a political project.

- On July 29, Researcher-2 emailed Researcher-1 the data compiled by Tea Leaves [Durham provides no evidence that TE-1 was involved in

this exchange].

- On August 19, Researcher-1 queried Internet data maintained by TE-1's company [it is not clear but this suggests it was not the data turned over to the University] for the aforementioned mail1.trump-email.com domain. Researcher-1 then emailed TE-1 with the list of domains that had communicated with it, saying the list, "does not make much sense with the storyline you have."
- On August 20, Tea Leaves emailed Tech Exec-1, Researcher-1, and Researcher 2, stating that, "even if we found what [TE-1] asks us to find in DNS, we don't see the money flow, and we don't see the content of some message saying, 'send money here'." Tea Leaves then explained that one could fill out sales forms and cause them, "to appear to communicate with each other in DNS." Tea Leaves then noted that "it's just not the case that you can rest assured that Hillary's opposition research and whatever professional gov

and investigative journalists are also digging come up with the same things."

- On August 20, TE-1 clarified that the task was "indeed broad," and that,
    - Being able to provide evidence of *anything* that shows an attempt to behave badly in relation to this [Durham doesn't describe what the antecedent of "this" is], the VIPs would be happy. They're looking for a true story that could be used as the basis for closer examination.
- Still on August 20, seemingly distinguishing between that task and the Alfa Bank allegations, TE-1 said, "the prior hypothesis was all that they needed: mailserver dedicated or related to trump … and with traffic almost exclusively with Alfa was sufficient to do the job. … Trump has claimed he and his company have had NO dealings with .ru other than the failed Casino, and the Miss universe pageant. He claims

absolutely NO interaction with any financial institutions. So any potential like that would be jackpot." [Ellipses original]

- On August 21, TE-1 emailed the recipients [but not, apparently, Sussmann], urging them to do further research on Trump which would "given the base of a very useful narrative." He added that he didn't believe the trump-email.com domain was a secret communications channel but a "red herring," because the host was "a legitimate valid company," stating they could "ignore it, together with others that seem to be part of the marketing world."
- On August 22, Researcher-1 raised doubts about whether, using only the tools they were currently using, they could prove their hypothesis. Among the concerns raised is that they couldn't prove that "this is not spoofed [] traffic." [brackets original; bolded in the original]
- Later in or about August 2016 [on dates Durham doesn't provide], TE-1

exchanged emails with personnel from Fusion.

Sussmann drafts a white paper and (via unstated means) TE-1 gets Researchers 1 and 2 and Tea Leaves to review it

- Between September 5 and September 14, Sussmann drafted a white paper, generally billing his time to the Clinton Campaign, but on September 14, billing time to both Clinton and TE-1.
- 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."

Sussmann shares this and

other information with James Baker and—Durham claims—affirmatively lies about whether he is representing someone

- Both before the September 19 meeting and after it (notably in a September 12 meeting involving the NYTimes, in which Marc Elias also participated), Sussmann spoke to the press about what Durham credibly suggests was the Alfa Bank white paper. Sussmann billed this to Clinton.
- On September 19, Sussmann met with Baker and provided him with three white papers and a thumb drive with data. Durham doesn't actually make clear where all three of these came from.
- On September 19, Sussmann met with James Baker. Durham claims that "he stated falsely that he was not acting on behalf of any client" [which Durham cannot quote because there's no contemporaneous record], that he had been approached by multiple cyber experts [Durham doesn't say whether the three he named were Researcher 1, Researcher 2,

and Tea Leaves or other people, as seems to be the case], three white papers [which I may return to because this is another problematic spot in his story], and some of the data, which Durham calls "purported."

- Immediately after the September 19 meeting, Baker met with Bill Priestap whose notes read:
    - Michael Sussman[n] – Atty: Perkins Coie – said not doing this for any client
        - Represents DNC, Clinton Foundation, etc. []
        - Been approached by Prominent Cyber People (Academic or Corp. POCs), People like: [three names redacted]
- Durham substantiates a claim that Sussmann billed the meeting itself to Hillary to a description, "work and communications regarding confidential project," that does not, at least as he quotes it, mention a meeting

> with the FBI General Counsel at all.

Some of this — the reference to crafting a narrative and a storyline — is damning and validates my discomfort with the political nature of this project five years ago. Other parts of this emphasize the researchers' insistence on truth from at least parts of this effort. 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.

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. He claims Sussmann, Researcher 1 and 2, TE-1, and Tea Leaves drafted the white paper(s) shared with the FBI, but all he substantiates is a less than one hour review by everyone but Sussmann. He leaves out a great deal of detail about what Jean Camp and someone using the moniker Tea Leaves did and said, publicly, after the FBI meeting, which may totally undercut Durham's "narrative."

But other parts, even of the story that Durham tells, are problematic for his narrative. First, there is not (yet) the least hint that Tea Leaves — whom he calls "The Originator" — fabricated this data (or even packaged it up misleadingly, though I think there is evidence he did). Nor is there the least hint that TE-1 asked Tea Leaves to come up with the data. That part of the story is fundamentally important and Durham simply ignores it with that legally unnecessary — particularly given that Durham clearly labels this person as Tea Leaves — moniker "Originator," giving the anomalous forensic data a kind of virgin birth. And while two of the four tech experts described herein (there appear to be at least three others not

described) expressed some doubt about the meaning of it, none of them seems to have doubted that there was an anomaly in the Trump marketing server and Alfa Bank.

Based on this story, though, Durham insinuates Sussmann fed information that he, Sussmann, knew to be bullshit to the FBI on behalf of both Hillary and TE-1, and in so doing affirmatively hid that the bullshit "storyline" was designed to help Hillary which (he claims) would have led the FBI to treat it differently.

In spite of a lot of thus far extraneous details, that's the only crime he has alleged.

The existing case is remarkably weak

As a number of people have noted, as charged this is a remarkably weak case. Ben Wittes dedicates a section of his post on this indictment to those weaknesses. They are, succinctly:

- The evidence regarding the core allegation in the indictment pits Sussmann's word against James Baker's; there are no other witnesses.
- After the meeting with Baker, Sussmann repeatedly admitted under oath he was representing a client, a detail which could be exculpatory or inculpatory.
- Baker testified to Congress he did believe Sussmann was representing a client (meaning Baker will be used to discredit Baker, the one

witness to Sussmann's alleged lie).

- Even in Bill Priestap's nearly-contemporaneous notes which are the only documentation of Sussmann's comments, he describes Sussmann as Hillary's lawyer (including for the Clinton Foundation, which may be incorrect), so FBI knew full well that Sussmann represented Hillary.
- Priestap's notes may be inadmissible hearsay at trial.

The NYT article predicting these charges also claim Durham is conflating Sussmann's tracking of his hourly work with the actual money charged to the Hillary campaign.

> Moreover, internal billing records Mr. Durham is said to have obtained from Perkins Coie are said to show that when Mr. Sussmann logged certain hours as working on the Alfa Bank matter — though not the meeting with Mr. Baker — he billed the time to Mrs. Clinton's 2016 campaign.
>
> [snip]
>
> They are also said to have argued that the billing records are misleading because Mr. Sussmann was not charging his client for work on the Alfa Bank matter, but needed to show internally that he was working on something. He was discussing the matter with Mr. Elias and the campaign paid a flat monthly retainer to the firm, so Mr. Sussmann's hours did not result in any additional charges, they said.

There are a number of other ways that Sussmann's presumably well-funded defense will combat these charges. But as to the allegation buried amid all these details, Durham's evidence is weak.

Durham's materiality broadcasts his bid for a ConFraudUS conspiracy

But that's not what this is about.

Durham is not just alleging that Sussmann was hiding that he was working for Hillary. He is also claiming that Sussmann was at the same time representing TE-1 at that meeting. In the indictment, I think that's based on a single data point — that Sussmann billed TE-1's company for "communications regarding confidential project" on September 14. I'm not sure whether that makes the false statements case still weaker or stronger.

But it's a key part of where Durham obviously wants to go.

Not only are many of the details Durham included in the indictment irrelevant to the false statements charge, but if they were crimes by themselves, they would have been tolled under any five year statute of limitations already. There are only two conceivable purposes for including them in this indictment. First, to give the Alfa Bank Oligarchs more cause to sue more people, effectively a US prosecutor assisting Russians in cynical lawfare. Durham's investigation incorporates stuff the Oligarchs have already liberated, so is itself derivative of Russian lawfare. Effectively, that means that a prosecutor working for Bill Barr's DOJ pursued a prosecution that was complementary to an intelligence-related effort by foreigners who pay Kirkland & Ellis a lot of money. Sussmann will have real cause to question whether Brian Benczkowski (who recused from matters involving this aspect of Alfa Bank) or any other Kirkland & Ellis lawyer had a role in this strand of the

investigation.

Then there's the most obvious way to extend the statute of limitations on the events that happened in July and August 2016: to include them in a conspiracy that continued after those dates (and indeed, Durham refers to Elias, Researcher 1 and 2, and Tea Leaves in the way DOJ often uses to refer to charged or uncharged co-conspirators).

Given the extended statement Durham includes to explain why Sussmann's alleged lie is material under the charged statute, that's undoubtedly where Durham wants to head with his investigation.

> 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.

Don't get me wrong. This will clearly pass the incredibly low standard for materiality under existing precedent. Though Sussmann will surely make much of citing the invented standard Billy Barr used to try to dismiss the Mike Flynn prosecution, which first requires the investigation in question to be legitimate.

> The Government is not persuaded that the January 24, 2017 interview was conducted with a legitimate investigative basis and therefore does not believe Mr. Flynn's statements were material even if untrue. Moreover, we not believe that the Government can prove either the relevant false statements or their materiality beyond a reasonable doubt.
>
> [snip]
>
> In any event, there was no question at the FBI as to the content of the calls; the FBI had in its possession word-for-word transcripts of the actual communications between Mr. Flynn and Mr. Kislyak. See Ex. 5 at 3; Ex. 13. at 3. With no dispute as to what was in fact said, there was no factual basis for the predication of a new counterintelligence investigation. Nor was there a justification or need to interview Mr. Flynn as to his own personal recollections of what had been said. Whatever gaps in his memory Mr. Flynn might or might not reveal upon an interview regurgitating the content of those calls would not have implicated legitimate counterintelligence interests or somehow exposed Mr. Flynn as beholden to Russia.

If DOJ had no interest in figuring out whether Trump was undermining sanctions to pay off a quid pro quo, they sure as hell have no interest in launching a 3-year investigation to figure out the tie between these allegations and Hillary that was obvious to Priestap in real time, particularly given how quickly the FBI dismissed the allegations in 2017 and given that the allegations are not publicly known to have had a tie to their larger Russian investigation.

Still, while Durham will have no trouble proving Sussmann's claimed lie meets the standards of materiality, Durham's claims for it are ridiculous.

It's a load of horseshit that FBI would have treated this tip any differently — which amounted to investigating it, alerting the press there was nothing to it, then dismissing it pretty quickly, as far as is public — if they knew that Sussmann was formally being paid at that meeting by Hillary, if he in fact was. Priestap knew Sussmann was representing Hillary and said as much in the best evidence Durham has! In fact, FBI's warning to the NYT about this story in October could be presented as evidence that FBI already incorporated an assumption this came from Hillary.

Likewise, it's a load of horseshit that FBI couldn't know that the Bureau needed to ID the researchers behind the project. If I was able to figure that was important out before the 2016 election, and I did, then the experts at the FBI surely figured that out.

But what Durham's materiality statement emphasizes — what Durham claims Sussmann *intended to hide* with his claimed lie — is that, "researchers at a U.S.-based university … were receiving and analyzing Internet data in connection with a pending federal government cybersecurity research contract." That's the significance of ¶¶23a through e of the indictment, which describe how TE-1 provided data that included some from an Executive Branch office of the U.S. government, which his company

had obtained “as a sub-contractor in a sensitive relationship between the U.S. government and another company,” to the university at which Researcher 1 and 2 were working, and both with his university researcher allies and employees of his own company, he tasked people to research Donald Trump. Durham is suggesting that subset of data taints the whole pool that TE-1 shared, making it a Federal interest.

It’s not just that Durham is working on a theory that Sussmann deliberately dealt garbage to the FBI (which GOP sources also did on the Clinton Foundation) while trying to hide that fact. It’s that data originally sourced from the government was used in doing that research.

It’s actually the kind of argument that DOJ prosecutors typically succeed with. Except it’s all premised on proving that Sussman was trying to hide all this in his meeting with Baker. Even if the evidence surrounding the meeting weren’t so flimsy, this is another degree of motive that Durham is straining mightily to make.

Durham *needs* Sussmann to have lied, because a deliberate attempt to obscure the rest is necessary for his “storyline.” His evidence that Sussmann lied — much less, deliberately — is shoddy. But if he can’t get that, then his hopes for a larger “narrative” collapse.

The parts of the story Durham doesn’t tell

That becomes more clear when you consider some details that Durham doesn’t include in his indictment.

Two details that were public to everyone involved make it clear why Durham’s silence about the exact dates in July when this operation started is so corrupt.

On July 22, WikiLeaks published emails that were at the time believed and since have been confirmed by the FBI to have been hacked by

Russia. Durham hides the dates in July when many of these events transpired, but everything he includes suggests this activity post-dated the time when WikiLeaks published stolen emails and the entire security community in the US, surely including every researcher mentioned in this story, coalesced on the belief that Russia was the culprit. Durham refers to Russia's attack on Hillary (and therefore on the US) inaccurately as, "the hacking of its email servers by the Russian government" and "a hack" (the hack went well beyond just email and continued through the period of Sussmann's meeting with Baker). But, amazingly, Durham's "narrative" doesn't account for the fact that Hillary was targeted not just with an attack but with an information operation. And the timeline he presents here affirmatively hides that these events took place *after* the entire security community understood that there was an information operation aspect to the attack.

Then, on July 27, Trump gave a press conference in Florida where he said numerous things that make all the actions of Sussmann and others justifiable *on national security grounds*. First, Trump raised doubts about the Russian attribution of the DNC hack that, by that point in July, was the consensus among national security experts, undoubtedly including every tech expert mentioned in this indictment.

> I watched this guy Mook and he talked about we think it was Russia that hacked. Now, first of all was what was said on those that's so bad but he said I watched it. I think he was live. But he said we think it was Russia that hacked.
>
> And then he said – and this is in person sitting and watching television as I've been doing – and then he said could be Trump, yeah, yeah. Trump, Trump, oh yeah, Trump. He reminded me of John Lovitz for "Saturday Night Live" in the liar (ph) where he'd go yes, yes, I went

> to Harvard, Harvard, yes, yes. This is the guy, you have to see it. Yes, it could be Trump, yes, yes. So it is so farfetched. It's so ridiculous. Honestly I wish I had that power. I'd love to have that power but Russia has no respect for our country.
>
> And that's why – if it is Russia, nobody even knows this, it's probably China, or it could be somebody sitting in his bed. But it shows how weak we are, it shows how disrespected we are. Total – assuming it's Russia or China or one of the major countries and competitors, it's a total sign of disrespect for our country. Putin and the leaders throughout the world have no respect for our country anymore and they certainly have no respect for our leader. So I know nothing about it.

Trump then offered his bullshit explanation for why he wouldn't release his tax returns, framing it in terms of whether he had business ties to Russia.

> TRUMP: Because it's under order. And I'll release them when the audits completed. Nobody would release when it's under – I've had audits for 15 or 16 years. Every year I have a routine audit. I'm under audit, when the audits complete I'll release them. But zero, I mean I will tell you right now, zero, I have nothing to do with Russia, yes?

Trump then said the nation-state hack of his opponent wasn't the important thing, the content of the emails that were released was, thereby encouraging the press to participate in the information operation aspect of this attack.

> He already did something today where he said don't blame them, essentially, for your incompetence. Let me tell you, it's

> not even about Russia or China or whoever it is that's doing the hacking. It was about the things that were said in those e-mails. They were terrible things, talking about Jewish, talking about race, talking about atheist, trying to pin labels on people – what was said was a disgrace, and it was Debbie Wasserman Schultz, and believe me, as sure as you're sitting there, Hillary Clinton knew about it. She knew everything.

Trump then asked Russia to further hack his opponent.

> Russia, if you're listening, I hope you're able to find the 30,000 e-mails that are missing.

Trump then doubled down on the comment he made about his taxes, assuring the press that he had "zero" business ties with Russia.

> TRUMP: No, I have nothing to do with Russia, John (ph). How many times do I have say that? Are you a smart man? I have nothing to with Russia, I have nothing to do with Russia.
>
> And even – for anything. What do I have to do with Russia? You know the closest I came to Russia, I bought a house a number of years ago in Palm Beach, Florida.
>
> Palm Beach is a very expensive place. There was a man who went bankrupt and I bought the house for $40 million and I sold it to a Russian for $100 million including brokerage commissions. So I sold it. So I bought it for 40, I told it for 100 to a Russian. That was a number of years ago. I guess probably I sell condos to Russians, OK?
>
> QUESTION: (OFF-MIKE)

> TRUMP: Of course I can. I told you, other than normal stuff – I buy a house if I sold it to a Russian. I have nothing to do with Russia. I said that Putin has much better leadership qualities than Obama, but who doesn't know that?
>
> QUESTION: (OFF-MIKE)
>
> TRUMP: Of course not. I own the Trump organization. Zero, zero. Go ahead.

Trump then reiterated his claim that no one could attribute the DNC hack to Russia.

> TRUMP: No, but they seem to be, if it's Russians. I have no idea. It's probably not Russia. Nobody knows if it's Russia. You know the sad thing is? That with the technology and the genius we have in this country, not in government unfortunately, but with the genius we have in government, we don't even know who took the Democratic National Committee e-mails. We don't even know who it is.
>
> I heard this morning, one report said they don't think it's Russia, they think it might be China. Another report said it might be just a hacker, some guy with a 200 I.Q. that can't get up in the morning, OK? Nobody knows. Honestly they have no idea if it's Russia. Might be Russia. But if it's any foreign country, it shows how little respect they have for the United States. Yes, ma'am.

Finally, Trump also stated that he would consider lifting sanctions on Russia.

> QUESTION: I would like to know if you became president, would you recognize (inaudible) Crimea as Russian territory? And also if the U.S. would lift sanctions that are (inaudible)?

> TRUMP: We'll be looking at that. Yeah, we'll be looking.

Each of these comments, individually, would have raised eyebrows. The same comments, made by an American citizen, would equally have raised alarms among those committed to cybersecurity.

But for a presidential candidate to encourage the hostile nation-state information operation targeting his opponent, then *ask the hostile nation-state to further target her*, in conjunction with the repeated denials of any business ties to Russia raised real, legitimate questions about whether Trump was putting his own interests above the national security of the country.

You might excuse Durham for excluding this from his indictment because after all he was busy indicting a ham sandwich based on hearsay evidence he might be able to exclude these facts at trial. Except that an August 20 comment from TE-1 that Durham quotes in his indictment may be a direct reference to (and at the least incorporates knowledge of) this press conference.

> Trump has claimed he and his company have had NO dealings with .ru other than the failed Casino, and the Miss universe pageant. He claims absolutely NO interaction with any financial institutions. So any potential like that would be jackpot.

That is, Durham included what appears to be a reference to the July 27 press conference. 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.

The parts of the story Durham doesn't tell

And not only was it objectively reasonable to test whether Trump's claims to have "zero" business ties to Russia were false, but those suspecting that Trump was hiding such ties were, in fact, correct.

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.

But that was not the only thing that Trump had done by the date when a bunch of security researchers responded to anomalous forensic data to test whether Trump was hiding further ties to Russia's attack on Hillary Clinton.

In March, Trump hired Paul Manafort, a financially desperate political operative with close ties to a Russian intelligence officer, Konstantin Kilimnik, who (SSCI provided three redacted examples of) may have been involved in the hack-and-leak operation. In April, Manafort started leveraging his relationship with Trump to try to make money. In May, Manafort started regularly sending Kilimnik the campaign's internal polling data. All that happened before researchers started testing Trump's claims to have had no tie to Russia. On July 28, Kilimnik emailed Manafort to set up a meeting to talk about the future of Ukraine. Just days after the researchers started the inquiry, on August 2, Manafort met with Kilimnik to discuss carving up Ukraine in the same meeting where he described his strategy to win the election.

In April, an academic with close ties to Russia, Joseph Mifsud, told an unqualified braggart whom Trump had added to his team to pretend he had a foreign policy plan, George Papadopoulos, that Russia had thousands of Hillary's emails that

they intended to release to help Trump.

In May, according to Rick Gates' testimony, Roger Stone started claiming he had advance knowledge of what would become the WikiLeaks releases. On or about June 15, per Gates, Stone told him that "he had contact with Guccifer 2." According to a warrant affidavit targeting Stone, he searched Google on "Guccifer" before the Guccifer website went up that day. On June 23, Manafort called Stone and then the two old friends met for 30 minutes in the Trump cafeteria. On June 30, Stone spoke to Trump. According to multiple sources (including Michael Cohen), Stone knew of the DNC drop before it happened.

In June, Don Jr accepted a meeting with Natalia Veselnitskaya at which he believed he would get dirt on Hillary Clinton. At the meeting, Veselnitskaya asked Don Jr to end sanctions on Russia, and the candidate's son said his dad would reconsider it if he won.

In short, the researchers who, in the wake of Trump's damning comments, were testing whether Trump had lied about having ties to Russia, not only had objectively reasonable reasons to do that research. But their suspicions were proven correct, over and over again.

Durham describes the outcome of the FBI investigation into the allegations this way:

> The FBI's investigation of these allegations nevertheless concluded that there was insufficient evidence to support the allegations of a secret communications channel with Russian Bank-1. In particular, and among other things, the FBI's investigation revealed that the email server at issue was not owned or operated by the Trump Organization but, rather, had been administered by a mass marketing email company that sent advertisements for Trump hotels and hundreds of other clients.

Nothing here suggests the FBI disproved that this was an anomaly.

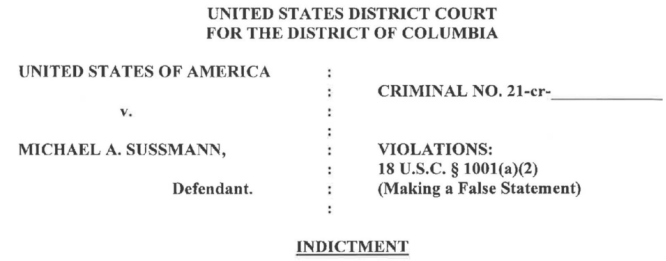
And there's one more detail that Durham didn't include in the Sussmann indictment: on July 26, Australia first shared their report about what George Papadopoulos told Alexander Downer in May. The next day, July 27, the FBI Legat in the UK got the tip. On July 31 — before the substantive research into the Alfa Bank allegation began — the FBI opened an UNSUB investigation into who got advance warning about the Russian operation and shared it with George Papadopoulos. In other words, by hiding the dates when Tea Leaves first discovered the anomalous data, Durham is hiding not just the damning things that publicly happened before the Alfa Bank operation got started, but probably details about the tip that turned into the Crossfire Hurricane investigation.

In the wake of the Sussmann indictment, the usual Russian denialists have claimed that this proves that what they call "Russiagate" was all a fraud.

With Clinton lawyer charged, the Russiagate scam is now indicted

In accusing Clinton campaign lawyer Michael Sussmann of lying to the FBI, Special Counsel John Durham offers new evidence of the fabrications behind the Trump-Russia conspiracy theory.

Aaron Maté
Sep 20 ♡ 90 💬 26



UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	CRIMINAL NO. 21-cr-_____
v.	:	
	:	
MICHAEL A. SUSSMANN,	:	VIOLATIONS:
	:	18 U.S.C. § 1001(a)(2)
Defendant.	:	(Making a False Statement)
	:	

INDICTMENT

The indictment of Hillary Clinton attorney Michael Sussmann offers new evidence that the Trump-Russia conspiracy theory that engulfed Trump's term in office was itself the product of fabrications involving Clinton's 2016 campaign.

Such claims defy the rules of physics, suggesting that events that happened after the FBI opened an investigation to learn how and why the Trump campaign (via three channels, as it

turns out) learned of the Russian attack in advance were in fact the cause of it.

It is likely that Durham will be able to exclude all these details from a Michael Sussmann trial, at least if it remains just a false statements case. He will be able to convince Judge Christopher Cooper, who is presiding over the case, that this information — that the researchers not only had reason to believe Trump presented a cybersecurity risk to the country, but that the researchers turned out to be right, and that FBI had itself determined there was reason to carry out the same kinds of investigations that the researchers did, possibly before any one of them took a single step — is irrelevant to the case against Sussmann. But if Durham charges ConFraudUS based on a claim that it was illegitimate to look into why Donald Trump was inviting Russia to hack his opponent, it will become centrally important that, before these researchers started conducting their investigation, the FBI had likewise decided such an investigation had merit.

The Alfa Bank story was sleazy and unethical. But it was still, nevertheless, an instance where someone representing the victim of a nation-state attack attempted to chase down information that may have pertained to that nation-state attack.

John Durham will go down in history as the guy who decided that torturing detainees, even in excess of legal guidance, was not a crime, but a victim sharing concerns about nation-state hacking is.

Update: It's likely that Richard Burt was one of the people investigated as part of this effort. Per the Mueller Report, he was the person Petr Aven asked to establish a tie with Trump's transition in 2016.

> After the December 2016 all-hands meeting, A ven tried to establish a connection to the Trump team. A ven

> instructed Richard Burt to make contact with the incoming Trump Administration. Burt was on the board of directors for LetterOne (L 1), another company headed by Aven, and had done work for Alfa-Bank. 1169 Burt had previously served as U.S. ambassador to Germany and Assistant Secretary of State for European and Canadian Affairs, and one of his primary roles with Alfa-Bank and Ll was to facilitate introductions to business contacts in the United States and other Western countries. 1170
>
> While at a L1 board meeting held in Luxembourg in late December 2016, Aven pulled Burt aside and told him that he had spoken to someone high in the Russian government who expressed interest in establishing a communications channel between the Kremlin and the Trump Transition Team. 1171 Aven asked for Burt's help in contacting members of the Transition Team. 1172 Although Burt had been responsible for helping Aven build connections in the past, Burt viewed Aven's request as unusual and outside the normal realm of his dealings with Aven. 1173
>
> Burt, who is a member of the board of CNI (discussed at Volume I, Section IV.A.4, supra), 1174 decided to approach CNI president Dimitri Simes for help facilitating A ven' s request, recalling that Simes had some relationship with Kushner. 1175 At the time, Simes was lobbying the Trump Transition Team, on Burt's behalf, to appoint Burt U.S. ambassador to Russia.1176
>
> Burt contacted Simes by telephone and asked if he could arrange a meeting with Kushner to discuss setting up a high-level communications channel between Putin and the incoming Administration.

> 1177 Simes told the Office that he declined and stated to Burt that setting up such a channel was not a good idea in light of the media attention surrounding Russian influence in the U.S. presidential election. 1178 According to Simes, he understood that Burt was seeking a secret channel, and Simes did not want CNI to be seen as an intermediary between the Russian government and the incoming Administration. 1179 Based on what Simes had read in the media, he stated that he already had concerns that Trump's business connections could be exploited by Russia, and Simes said that he did not want CNI to have any involvement or apparent involvement in facilitating any connection. 118

Update: Corrected scope of Benczkowski's recusal. His should cover the server issue (and Alfa Bank issues for the first two years he was CRM).

Update: Brian Krebs wrote a post laying out all the people who still believe there's something going on technically. I don't think that's inconsistent, at all, with this one. As noted, everyone who looked at this believes it's an anomaly. What I keep pointing to is the aftermath of that anomaly got Alfa Bank to act in a certain way that is consistent with Putin's interests. Krebs notes that it has also led to a lot of scrutiny of security researchers in the US, not unlike the way the aftermath of the Steele dossier discredited most top Russian experts in the US government.

Update: This transcript of Preet Bharara and Joyce Vance discussing the many weaknesses of the Durham indictment largely replicates what I've laid out here but is worth a review.