THE TRIPARTITE (AT LEAST) STRUCTURE OF THE RUSSIAN HACK INVESTIGATION

As I mentioned in this post, on Saturday, Reuters offered the most comprehensive description of the structure of the FBI investigation into the DNC hack. As it describes there are "at least" three different distinct probes into the FBI hack: one led by counterintelligence agents based in DC, one in Pittsburgh targeted at the hack of the DNC itself, and one in San Francisco targeted at the Guccifer 2 persona.

That structure is interesting for a number of reasons, not least that, in recent years, FBI has assigned cyber investigative teams to geographical offices that have developed certain expertise. I'm most interested that FBI has split the Guccifer 2 side of the investigation off from the hack of the DC.

DC: The Counterintelligence investigation

Let's start with the DC investigation. Contrary to what you may think, a good deal of the attention on Trump's close advisors stems from behavior that barely involves the DNC hack, if at all, but instead focuses on larger discussions of quid pro quo. Here's what has been publicly alleged, mostly in the Trump dossier. Reminder, these are only allegations!

> Paul Manafort, using Carter Page as a go between, conducts on-going quid pro quo about attacks on Hillary in response for distracting from Ukraine issues. (PDF 8)
>
> Carter Page conducts a meeting with

> Rosneft CEO (and US sanction target) Igor Sechin in Moscow. The two discuss a quid pro quo tying 19% transfer of Rosneft to Page in exchange for the lifting of sanctions.(PDF 9, 30) On the same visit, Page meets top Kremlin official Diyevkin, where the latter explains to Page what kind of compromising information they had on both Trump and Hillary. (PDF 9)
>
> A Kremlin figure describes Russian efforts to reach out to some in the US, including Jill Stein, Mike Flynn, and Carter Page. (PDF 15)
>
> At a meeting in August, Yanukovych admits to Putin that he had paid off Manafort, but had covered it up. According to Steele's sources, Putin doubts how well Yanukovych had covered his tracks. (PDF 20-21)
>
> Trump lawyer Michael Cohen meets with Russian Presidential Administration figures, including Oleg Solodukhin, operating under the cover of the Rossotrudnichestvo organization, in Prague in August. According to two pre-election reports, this meeting was to clean up fall-out of prior contacts with Manafort (here described exclusively in terms of his involvement in Ukraine) and Page (described as the quid pro quo on sanctions). (PDF 18, 31-32) According to a post-election report, the meeting also discusses payments and cover-up of Europe-based hackers, who would be paid by both the Russians and Trump. (PDF 34-35) The role of Cohen – whose wife is Russian and whose father-in-law is a key Russian developer – as liaison to Russia is key. Note, information likely indicating intelligence sourcing is redacted in two of these reports. (PDF 30, 34)

The one other Trump figure mentioned in allegations of Russian ties, Roger Stone, is not mentioned in the dossier, though his role has exclusively been described as a potential knowing go-between with Wikileaks. (The error I mentioned I made in my the OTM interview was in forgetting Cohen, whose role is central, and instead mentioning Stone.)

In other words, while allegations of involvement with Russia do touch on the DNC hack, for both Manafort and Page, the evidence focuses more on old-fashioned influence peddling. The evidence against Flynn *in the dossier* is exclusively that of cultivation.

Only Cohen, though, is strongly and repeatedly alleged in the dossier to have had a role in both the influence peddling and arranging — and paying! — for the DNC hack (though a weak allegation against Manafort is made in an early report).

Yesterday, NYT reported that Cohen tried to pitch a crazy "peace" deal for Ukraine to Mike Flynn not long before the latter was caught on an intercept with Russia's Ambassador.

> A week before Michael T. Flynn resigned as national security adviser, a sealed proposal was hand-delivered to his office, outlining a way for President Trump to lift sanctions against Russia.
>
> Mr. Flynn is gone, having been caught lying about his own discussion of sanctions with the Russian ambassador. But the proposal, a peace plan for Ukraine and Russia, remains, along with those pushing it: Michael D. Cohen, the president's personal lawyer, who delivered the document; Felix H. Sater, a business associate who helped Mr. Trump scout deals in Russia; and a Ukrainian lawmaker [named Andrii Artemenko].

Note that Sater, who has mobbed up business ties

with Trump the latter has denied, also allegedly has worked for the CIA.

All of this is a way of saying that several of Trump's advisors — especially Cohen — have been alleged to have dodgy ties to Russian, but much if not most of that pertains to influence peddling tied to Ukraine and sanctions imposed in retaliation for Russian involvement in Ukraine. So even beyond the different technical and security requirements of the investigation (not to mention any sensitivity involving the CIA), such an investigation sensibly would reside in FBI's CI world. Thus the DC investigation.

Pittsburgh: The DNC hackers

As Reuters describes it, the Pittsburgh inquiry is examining who hacked the DNC (curiously, it makes no mention of John Podesta or any other hack target).

> The FBI's Pittsburgh field office, which runs many cyber security investigations, is trying to identify the people behind breaches of the Democratic National Committee's computer systems, the officials said. Those breaches, in 2015 and the first half of 2016, exposed the internal communications of party officials as the Democratic nominating convention got underway and helped undermine support for Hillary Clinton.
>
> The Pittsburgh case has progressed furthest, but Justice Department officials in Washington believe there is not enough clear evidence yet for an indictment, two of the sources said.

It's not just that Pittsburgh conducts a lot of cyber security investigations — though it has been involved in some key multinational cybercrime investigations (and perhaps as

importantly, infrastructure take-downs). In addition to international partnerships in those investigations, it partners closely with Carnegie Mellon's CERT, which is best known for developing an attack on Tor the FBI uses (the legal follow-up to the 2014 Operation Onymous operation that exposed it went through SDNY in Manhattan, though that would have been before FBI started assigning investigations by geography).

Pittsburgh is also where the most discussed indictment of a nation-state hacking group — that of Chinese People's Liberation Army hackers, mostly for spying on negotiations — came through (most of the victim companies were there too, but that was probably because they could all serve as victims without compromising national security). I will be interested to see whether the FBI assigned this investigation to Pittsburgh before or after Crowdstrike declared the DNC hack a state-sponsored hack.

San Francisco: Guccifer 2

Finally, there is the investigation into Guccifer 2, the persona who claimed to have hacked the DNC, who took credit for handing the documents to WikiLeaks, and who allegedly had ties to DC Leaks. Here's how Reuters describes this part of the investigation:

> Meanwhile the bureau's San Francisco office is trying to identify the people who called themselves "Guccifer 2" and posted emails stolen from Clinton campaign manager John Podesta's account, the sources said. Those emails contained details about fundraising by the Clinton Foundation and other topics.

The language here is really curious.
The *strongest* case that Russia's GRU hacked a Democratic target involves Podesta. And Guccifer didn't post any Podesta emails. Guccifer claimed

to have posted Clinton Foundation documents, though the documents appeared to be DCCC documents, my comment on which elicited an unsolicited response from Guccifer.

Reuters is actually not the first outlet to report that San Francisco was investigating Guccifer. I believe credit for that goes to Ellen Nakashima's report, the day before Obama imposed sanctions, on how the US might retaliate.

> Criminal indictments of Russians might become an option, officials said, but the FBI has so far not gathered enough evidence that could be introduced in a criminal case. At one point, federal prosecutors and FBI agents in San Francisco considered indicting Guccifer 2.0, a nickname for a person or people believed to be affiliated with the Russian influence operation and whose true identity was unknown.

In December, at least, it appears the FBI did not know Guccifer's identity though they still believed it to be tied to Russia. Nevertheless that part of the investigation had already been spun out to San Francisco, the other side of the country from the Pittsburgh hack investigation.

Now, there have always been reasons to doubt the interpretation that Russian metadata invoking Felix Dzerzhinsky was proof that Guccifer was Russian, rather than disinformation casting blame on Russia. Here are two more recent pieces making that argument. And in Guccifer's most recent posting — posted on January 12 but fairly obviously written and posted in advance — the persona used proper English. Nevertheless, that's presumably not why this part of the investigation got spun off.

There are several other possibilities explaining why the Guccifer investigation is in San Francisco. That office, too, does a ton of cyber investigations, but virtually all of those

involve Bay Area companies targeted as victims. So it's possible the San Francisco office is leading the investigation because of some tie with an area company. Guccifer posted on WordPress, which is headquartered in San Francisco, so that could explain it. It's also possible FBI believes there is a tie between Guccifer and Shadow Brokers. The latter persona is not mentioned by Reuters, but they are surely also being investigated, perhaps even separately from the Hal Martin investigation in Maryland. If that's the case, the victim American firewall companies exposed in the first release are all headquartered in Silicon Valley (though they were initially victimized by NSA's TAO hackers, unless the companies knew NSA was using those back doors).

There are two other interesting cases that might suggest why the Guccifer part of the investigation is out in San Francisco. First, the corrupt government agents who stole Bitcoin while they were investigating Silk Road were investigated and tried out there. I've always suspected that was done to make it harder for Ross Ulbricht to access information on that investigation in discovery (if that was the intent, it worked like a charm!).
I'm *not* suggesting there's anything like that going on here, but I can imagine reasons why the FBI might want to firewall some parts of this investigation from others.

Finally, note that Yevgeniy Aleksandrovich Nikulin, the credential theft hacker arrested in Prague in October, was investigated out of San Francisco, explicitly because his alleged victims are also located in the Bay Area. There have always been hints that that arrest might tie into the Russian investigation (not least because Nikulin is Russian), but this would seem to suggest there's a tangential tie to it. So perhaps by the time FBI split up this investigation that theory had been developed.

Update: Laura Rozen reminds me via Twitter that Russia's San Francisco Consulate was one of the

locales from which diplomats were expelled.

A final comment. As interesting as it is that this investigation has split into three, I find it just as interesting that EDVA is *not* involved in it, which is where most international hacking investigations take place. I've got no explanation for why *that* might be, but it is as interesting a question as why the Guccifer investigation got sent out to San Francisco.

One thing is clear, though: For some reason, FBI thought it best to split two parts of what have widely believed to have been part of the same operation — the hacking and (some of) the leaking — and conduct them completely across the country from each other.