2018 SENATE INTELLIGENCE GLOBAL THREAT HEARING TAKEAWAYS

Today was the annual Senate Intelligence Committee Global Threat Hearing, traditionally the hearing where Ron Wyden gets an Agency head to lie on the record.

That didn't happen this time.

Instead, Wyden gave FBI Director Christopher Wray the opportunity to lay out the warnings the FBI had given the White House about Rob Porter's spousal abuse problems, which should have led to Porter's termination or at least loss of access to classified information.

> The FBI submitted a partial report on the investigation in question in March. And then a completed background investigation in late July. That, soon thereafter, we received request for follow-up inquiry. And we did that follow-up and provided that information in November. Then we administratively closed the file in January. And then earlier this month we received some additional information and we passed that on as well.

That, of course, is the big takeaway the press got from the hearing.

A follow-up from Martin Heinrich shortly after Wyden's question suggested he had reason to know

of similar “areas of concern” involving Jared Kushner (which, considering the President’s son-in-law is under investigation in the Russian investigation, is not that surprising). Wray deferred that answer to closed session, so the committee will presumably learn some details of Kushner’s clearance woes by the end of the day.

Wray twice described the increasing reliance on “non-traditional collectors” in spying against the US, the second time in response to a Marco Rubio question about the role of Chinese graduate students in universities. Rubio thought the risk was from the Confucius centers that China uses to spin Chinese culture in universities. But not only did Wray say universities are showing less enthusiasm for Confucius centers of late, but made it clear he was talking about “professors, scientists, and students.” This is one of the reasons I keep pointing to the disproportionate impact of Section 702 on Chinese-Americans, because of this focus on academics from the FBI.

Susan Collins asked Mike Pompeo about the reports in The Intercept and NYT on CIA’s attempts to buy back Shadow Brokers tools. Pompeo claimed that James Risen and Matt Rosenberg were “swindled” when they got proffered the story, but along the way confirmed that the CIA was trying to buy stuff that “might have been stolen from the US government,” but that “it was unrelated to this idea of kompromat that appears in each of those two articles.” That’s actually a confirmation of the stories, not a refutation of them.

There was a fascinating exchange between Pompeo and Angus King, after the latter complained that, “until we have some deterrent capacity we are going to continue to be attacked” and then said right now there are now repercussions for Russia’s attack on the US.

> Pompeo: I can’t say much in this setting I would argue that your statement that we have done nothing does not reflect the responses that, frankly, some of us

> at this table have engaged in or that this government has been engaged in both before and after, excuse me, both during and before this Administration.
>
> King: But deterrence doesn't work unless the other side knows it. The Doomsday Machine in Dr. Strangelove didn't work because the Russians hadn't told us about it.
>
> Pompeo: It's true. It's important that the adversary know. It is not a requirement that the whole world know it.
>
> King: And the adversary does know it, in your view?
>
> Pompeo: I'd prefer to save that for another forum.

Pompeo later interjected himself into a Kamala Harris discussion about the Trump Administration's refusal to impose sanctions by suggesting that the issue is Russia's response to cumulative responses. He definitely went to some effort to spin the Administration's response to Russia as more credible than it looks.

Tom Cotton made two comments about the dossier that Director Wray deferred answering to closed session.

First, he asked about Christopher Steele's ties to Oleg Deripaska, something I first raised here and laid out in more detail in this Chuck Grassley letter to Deripaska's British lawyer Paul Hauser. When Cotton asked if Steele worked for Deripaska, Wray said, "that's not something I can answer." When asked if they could discuss it in a classified setting, Wray said, "there might be more we could say there."

Cotton then asked if the FBI position on the Steele dossier remains that it is "salacious and unverified" as he (misleadingly) quoted Comey as saying last year. Wray responded, "I think

there's maybe more we can talk about this afternoon on that." It's an interesting answer given that, in Chuck Grassley's January 4 referral, he describes a "lack of corroboration for [Steele's dossier] claims, at least at the time they were included in the FISA applications," suggesting that Grassley might know of corroboration since. Yet in an interview by the even better informed Mark Warner published 25 days later, Warner mused that "so little of that dossier has either been fully proven or conversely, disproven." Yesterday, FP reported that BuzzFeed had hired a former FBI cybersecurity official Anthony Ferrante to try to chase down the dossier in support of the Webzilla and Alfa bank suits against the outlet, so it's possible that focused attention (and subpoena power tied to the lawsuit) may have netted some confirmation.

Finally, Richard Burr ended the hearing by describing what the committee was doing with regards to the Russian investigation. He (and Warner) described an effort to bring out an overview on ways to make elections more secure. But Burr also explained that SSCI will release a review of the ICA report on the 2016 hacks.

> In addition to that, our review of the ICA, the Intel Committee Assessment, which was done in the F—December of 06, 16—we have reviewed in great detail, and we hope to report on what we found to support the findings where it's appropriate, to be critical if in fact we found areas where we found came up short. We intend to make that public. Overview to begin with, none of this would be without a declassification process but we will have a public version as quickly as we can.

Finally, in the last dregs of the hearing, Burr suggested they would report on who colluded during the election.

> We will continue to work towards

> conclusions on any cooperation or collusion by any individual, campaign, *or company* with efforts to influence elections or create societal chaos in the United States.

My impression during the hearing was that this might refer to Cambridge Analytica, which tried to help Wikileaks organize hacked emails — and it might well refer to that. But I wonder if there's not another company he has in mind.

GRAHAM AND GRASSLEY ARE SEEING CHRISTOPHER STEELE'S GHOST WHERE MIKE FLYNN LURKS

Chuck Grassley and Lindsey Graham have gotten so paranoid about Christopher Steele they're seeing him where Mike Flynn probably really lurks.

THE TIMING OF MARK WARNER'S PSEUDOSCANDAL TEXTS

The Mark Warner texts that Fox just reported on, a week after Julian Assange promised news on Mark Warner to Sean Hannity, date to around the period of a massive T-Mobile hack in the DC area last year.

WHY CALL ALICE DONOVAN A TROLL?

Both WaPo and CounterPunch describe how a Russian persona published at CP and others. But why do they call the persona a troll?

WHY IS RUSSIA FINALLY LETTING (DUBIOUS) DETAILS OF ITS INVOLVEMENT IN DNC HACK OUT?

There’s a bunch of new claims out of Russia about hackers involved in the DNC hack. The reports are as interesting for the timing as for the claims made in them.

THREE MONTHS AFTER PROBLEMATIC JOHN SIPHER POST, JUST SECURITY MAKES CLEAR IT LET KNOWN ERRORS

SIT FOR TWO MONTHS

Just Security let significant errors go uncorrected for two months in a very prominent post because they didn't like that I had identified the errors in real time.

ABBE LOWELL REVEALS THE COMPLETE INADEQUACY OF THE INTELLIGENCE COMMITTEE RUSSIAN INVESTIGATIONS

In his contemptuous response to Dianne Feinstein's request that he actually comply with the Senate Judiciary Committee's earlier request for documents, Jared Kushner's lawyer, Abbe Lowell, says things that make it clear the Intelligence Committee investigations into Russian tampering with the election are totally inadequate.

THE IMPLICIT THREAT IN JULIAN ASSANGE'S AMBASSADOR TWEET

Julian Assange's tweet offering to set up a luxury immunity suite hotel in DC is a pretty explicit threat, one using the CIA as hostage.

AT SOME POINT TRUMP'S DENIALS ARE ABOUT CRIMINAL DEFENSE, NOT JUST DENIAL

After chatting up Putin, Trump backed Putin's version of the hack of last year's election again today. At this point, I think this is more about criminal defense than plain old denial.

ABOUT THE TIMING OF THE BINNEY MEETING

The Intercept is reporting that, on Trump's orders, Mike Pompeo met with Bill Binney on October 24 to understand his theory arguing that the DNC hack was in fact a leak.

> In an interview with The Intercept, Binney said Pompeo told him that President Donald Trump had urged the CIA director to meet with Binney to discuss his assessment that the DNC data theft was an inside job. During their hour-long meeting at CIA headquarters, Pompeo said Trump told him that if Pompeo "want[ed] to know the facts, he should talk to me," Binney said.
>
> [snip]
>
> Binney said that Pompeo asked whether he would be willing to meet with NSA and FBI officials to further discuss his analysis of the DNC data theft. Binney

> agreed and said Pompeo said he would contact him when he had arranged the meetings.

I've got a few comments about this.

First, I'm particularly intrigued in the timing. on Twitter, Jim Sciutto said Trump had been pushing for Pompeo to meet with Binney for several weeks.

> Pompeo took the meeting at the urging of President Trump over weeks. Pompeo told Binney: "The president told me I should talk to you"

I've been told the meeting was set up by October 14, which means Trump has been pushing for this meeting for over a month. That dates it to around the same time as reports that Chief of Staff John Kelly was preventing Dana Rohrabacher from meeting Trump to pass on Julian Assange's claims explaining how the emails he received didn't come from Russia, though that scheme went back further, to mid-August.

Effectively, though, that means Trump has been trying to find some way to magnify theories that argue culprits besides Russia did the hack. The guy who begged Russia to hack Hillary's emails in the middle of last summer is looking for some alternative narrative to push, and it's not clear whether he cares what that narrative is.

Though, as I noted in my post on these theories, now that we know the files Guccifer 2.0 leaked were from Podesta and as-yet unidentified sources, it makes all the arguments focusing on Guccifer beside the point (and disrupts Craig Murray's claims).

> On top of a lot of other implications of this, it shifts the entire debate about whether Guccifer 2.0 was WikiLeaks' source, which has *always* focused on whether the documents leaked on July 22 came from Guccifer 2.0. Regardless of

> what you might conclude about that, it shifts the question to whether the Podesta emails WikiLeaks posted came from Guccifer 2.0, because those are the ones where there's clear overlap. Russia's role in hacking Podesta has always been easier to show than its role in hacking the DNC.
>
> It also shifts the focus away from whether FBI obtained enough details from the DNC server via the forensic image it received from Crowdstrike to adequately assess the culprit. Both the DNC and Hillary (as well as the DCCC) servers are important. Though those that squawk about this always seem to miss that FBI, via FireEye, disagreed with Crowdstrike on a key point: the degree to which the two separate sets of hackers coordinated in targeted servers; I've been told by someone with independent knowledge that the FBI read is the correct one, so FBI certainly did their own assessment of the forensics and may have obtained more accurate results than Crowdstrike (I've noted elsewhere that public IC statements make it clear that not all public reports on the Russian hacks are correct).
>
> In other words, given that the files that Guccifer 2.0 first leaked actually preempted WikiLeaks' release of those files by four months, what you'd need to show about the DNC file leaks is something entirely different than what has been shown.

Binney and the other skeptics aren't even arguing the right issue anymore.

Moreover, there's a newly public detail that may moot two key strands of the argument. Last week the WSJ (here's the Reuters version) reported that DOJ is thinking of charging 6 Russian officials in the hack of the DNC. I get it.

People are skeptical that the FBI has any better data than the NSA (though I know others, outside of the FBI, believe they've pinpointed hackers by name). But as part of that story, they described the four districts where the investigation into the hack (as distinct from Mueller's investigation into the election tampering) live.

> The U.S. Justice Department has gathered enough evidence to charge six members of the Russian government in the hacking of Democratic National Committee computers before the 2016 U.S. presidential election, the Wall Street Journal reported on Thursday, citing people familiar with the investigation.
>
> Federal agents and prosecutors in Washington, Philadelphia, Pittsburgh and San Francisco have been cooperating on the DNC investigation and prosecutors could bring the case to court next year, it said.
>
> [snip]
>
> The hacking investigation, conducted by cybersecurity experts, predates the appointment in May of federal special counsel Robert Mueller to oversee the probe of alleged Russian meddling in the 2016 election and possible collusion with President Donald Trump's campaign.
>
> Mueller and the Justice Department agreed to allow the technical cyber investigation to continue under the original team of agents and prosecutors, the Journal said.

I'm not sure the report is 100% accurate; for example, I know of a non-political witness in the election-related hack being interviewed by Mueller's people.

But it includes a little-noticed detail that I know to be accurate — and important to rebut the

claim that the copying speed claimed by Forensicator requires a conclusion incompatible with Russia carrying out the hack. Part of the investigation is in Philadelphia.

When Reuters first reported a tripartite structure of the investigation in February, it included San Francisco (the Guccifer 2.0 investigation), Pittsburgh (the Russian side, probably focused on known APTs), and DC (the counterintelligence side — though that would significantly be Mueller's investigation).

Philadelphia was not included. I only know a bit about the Philadelphia side of the investigation, but I do know that part of the investigation is located there because of a server in the district. So one way or another, we know that the FBI is conducting an investigation in an Eastern city as part of the hacking investigation based on the use of a server in the district. That doesn't necessarily mean they're investigating Russians. But it means even if you account for a server in the eastern time zone, you still have FBI preparing to charge Russians for the hack.

Which brings us to the last line of the Intercept article.

> Binney said that since their meeting, he has not heard from Pompeo about scheduling follow-up meetings with the NSA and FBI.

Granted, it has only been two weeks. But in that time, not even Pompeo's prodding has made the FBI (more likely) or the NSA (which still has bad blood with Binney) remotely curious about these theories.