THE TIMING OF MARK WARNER'S PSEUDOSCANDAL TEXTS

By now, you've heard about Fox News' scoop that Mark Warner made efforts last year to obtain testimony from two key figures in the Senate Intelligence Committee investigation into Russia's involvement in the 2016 election via DC fixer Adam Waldman: Christopher Steele and Oleg Deripaska. (In my opinion, the news buried at the bottom of the story that Deripaska agreed to provide testimony if he could get immunity, but did not get it, is far more interesting than the rest of this, but I'm not a Fox News editor.)

> "We have so much to discuss u need to be careful but we can help our country," Warner texted the lobbyist, Adam Waldman, on March 22, 2017.
>
> "I'm in," Waldman, whose firm has ties to Hillary Clinton, texted back to Warner.

The story also includes this paragraph, which also has gotten less attention.

> Warner began texting with Waldman in February 2017 about the possibility of helping to broker a deal with the Justice Department to get the WikiLeaks founder Julian Assange to the United States to potentially face criminal charges. That went nowhere, though a Warner aide told Fox News that the senator shared his previously undisclosed private conversations about WikiLeaks with the FBI.

Interestingly, the Fox story relies on texts that Warner and Richard Burr jointly requested in June (targeting Waldman's phone, not Warner's, apparently), and then turned over to

the committee in October. I look forward to seeing how the notoriously anti-leak Burr deals with the apparent leak of committee sensitive materials to the right wing press.

Even while the story links to texts from SSCI, it comes a week after a woman duped the famously paranoid Julian Assange into exchanging texts with her fake Sean Hannity account promising news on Mark Warner.

> [Dell] Gilliam, a technical writer from Texas, was bored with the flu when she created @SeanHannity__ early Saturday morning. The Fox News host's real account was temporarily deleted after cryptically tweeting the phrase "Form Submission 1649 | #Hannity" on Friday night. Twitter said the account had been "briefly compromised," according to a statement provided to The Daily Beast, and was back up on Sunday morning.
>
> [snip]
>
> Just minutes after @SeanHannity disappeared, several accounts quickly sprung up posing as the real Hannity, shouting from Twitter exile. None were as successful as Gilliam's @SeanHannity__ account, which has since amassed over 24,000 followers.
>
> Gilliam then used her newfound prominence to direct message Assange as Hannity within hours.
>
> "I can't believe this is happening. I mean… I can. It's crazy. Nothing can be put past people," Gilliam, posing as Hannity, wrote to Assange. "I'm exhausted from the whole night. What about you, though? You doing ok?"
>
> "I'm happy as long as there is a fight!" Assange responded.
>
> Gilliam reassured Assange that she, or Hannity, was also "definitely up for a

> fight" and set up a call for 9:30 a.m. Eastern, about six hours later.
>
> "You can send me messages on other channels," said Assange, the second reference to "other channels" he made since their conversation began.
>
> "Have some news about Warner."

With that in mind, I want to look at the timing of some security issues last year.

While the texts turned over to Congress date to February 14, the conversation pertaining to Steele started around March 22. That puts it not long after news of a massive hack involving T-Mobile, first reported March 16.

> An unusual amount of highly suspicious cellphone activity in the Washington, D.C., region is fueling concerns that a rogue entity is surveying the communications of numerous individuals, likely including U.S. government officials and foreign diplomats, according to documents viewed by the *Washington Free Beacon* and conversations with security insiders.
>
> A large spike in suspicious activity on a major U.S. cellular carrier has raised red flags in the Department of Homeland Security and prompted concerns that cellphones in the region are being tracked. Such activity could allow pernicious actors to clone devices and other mobile equipment used by civilians and government insiders, according to information obtained by the *Free Beacon*.
>
> It remains unclear who is behind the attacks, but the sophistication and amount of time indicates it could be a foreign nation, sources said.

I would hope to hell that former cell company mogul and current Ranking Member on the Senate

Intelligence Committee running an important counterintelligence investigation Mark Warner would be aware of the security problems with mobile phones. But what do I know? **[Update: Not much. Looking more closely it looks like he was using Signal.]** In the last several months we've learned that FBI's investigators discuss the even more sensitive aspects of the more important side of counterintelligence investigation on SMS texts on their Samsung cell phones.

¯_(□)_/¯

But who knows what Waldman (who apparently chats a lot with spies, mobbed up Russian oligarchs, and — as Mike Pompeo deemed Wikileaks — non-state hostile intelligence services) knows about cell phone security?

In any case, the day before that was reported publicly, Ron Wyden and Ted Lieu sent a letter to John Kelly (who, as a reminder, in spite of or because he ran DHS for a while, had his own cell phone compromised), stating in part,

> We are also concerned that the government has not adequately considered the counterintelligence threat posed by SS7-enabled surveillance.
>
> [snip]
>
> What resources has DHS allocated to identifying and addressing SS7-related threats? Are these resources sufficient to protect U.S. government officials and the private sector.

If the government started considering such issues in March, they might have gotten around to discovering what kinds of problems were created by the T-Mobile hack in June, when Warner and Burr moved to get the texts for SSCI.

In any case, at around that point in time, APT 28 (one of the entities blamed for hacking the DNC the previous year) started a phishing campaign targeting the Senate's email server.

> Beginning in June 2017, phishing sites were set up mimicking the ADFS (Active Directory Federation Services) of the U.S. Senate. By looking at the digital fingerprints of these phishing sites and comparing them with a large data set that spans almost five years, we can uniquely relate them to a couple of Pawn Storm incidents in 2016 and 2017. The real ADFS server of the U.S. Senate is not reachable on the open internet, however phishing of users' credentials on an ADFS server that is behind a firewall still makes sense. In case an actor already has a foothold in an organization after compromising one user account, credential phishing could help him get closer to high profile users of interest.

Reporting at the time suggested this was an effort in advance of the 2018 election (which aside from minimizing the damage Russia might do in the interim, ignores the fact that staffers are ostensibly prohibited from using Senate resources for election related activities). But it always seemed to me it would more profitably target policy.

Or, maybe the only reasonable work Congress is doing to investigate the Russians?

Whether there's a connection between these two compromises last year or not, and Julian Assange, and this Mark Warner story, it's clear that DC remains ill-prepared to address the counterintelligence problems they're faced with.