HOW YEVGENIY NIKULIN MIGHT PLAY INTO THE MUELLER INVESTIGATION

For three reasons, Yevgeniy Nikulin, the Russian hacker alleged to be behind massive breaches of the LinkedIn and MySpace hacks, is in the news of late.

- The report that Michael Cohen was tracked traveling from Germany to Czech Republic in 2016 has raised questions about whether both Cohen and Nikulin were in Prague at the same time, Mohammed Atta-like
- Nikulin was suddenly extradited from Prague some weeks ago
- His (Russian-provided) lawyer says he'll entertain a plea deal

All of which provides a good opportunity to lay out what role he may have (or may be said to have) played in the DNC hack-and-leak.

The Michael Cohen in Prague story

The McClatchy report describing Robert Mueller receiving evidence of Cohen traveling from Germany to Czech Republic and some unknown date in 2016 seems to derive from outside investigators who have shared information with Mueller, not from Mueller's team itself (which is consistent with his locked down shop). As

such, it falls far short of being a confirmation of a meeting, or even validation that Mueller has confirmed any intelligence shared with his investigators. Moreover, the report has little detail as to timing, either of the visit or when Mueller actually got this intelligence.

And while it took a bit of time (Cohen can be forgiven for the delay because he apparently has very urgent business hanging with his homies smoking cigars), he did deny this report, offering the same partial story he offered last year.

That said, given the claimed timing, any coincidental presence in Prague by both Cohen and Nikulin is unlikely. Cohen's presence in Prague is said to have roughly aligned with that reported in the dossier, so August or September. According to the FBI's arrest affidavit for Nikulin he passed from Belarus into Poland on October 1, 2016, and probably was still there when posting from Warsaw on October 3; Nikulin was arrested in Prague on October 5. So unless Cohen went to Prague during his known October 2016 trip to England (definitely a possibility, but inconsistent with the dossier reporting), then they would no more have met in Prague (or planned to) than Mohammed Atta and Iraq's Ahmad Samir al-Ani did.

The sudden Nikulin extradition

That said, I do think the sudden Nikulin extradition, even as pro-Russian Czech President Milos Zeman fought with Czech Justice Minister Robert Pelikan over it — even to the point of threatening to replace him — is worth noting. That's true, first of all, because it appears Paul Ryan — purportedly on vacation with his family, but making appearances with everyone but Zeman — had a hand in it.

> During a visit to the Czech Republic, U.S. House Speaker Paul Ryan said on March 27 that "we have every reason to believe and expect that Mr. Nikulin will be extradited to America."
>
> "The United States has the case to prevail on having him extradited, whether it's the severity of the crime, which is clearly on the side of U.S., or the timing of the request for the extradition," he told reporters.
>
> In an interview with RFE/RL in Prague on March 26, Ryan said that the "case for extraditing [Nikulin] to America versus Russia is extremely clear."
>
> Ryan, who met with Prime Minister Andrej Babis and other Czech officials during his visit, told RFE/RL that he would raise the issue in those talks.
>
> "He did violate our laws, he did hack these companies…. So the extradition claim is very legitimate," he said. "And I just expect that the Czech system will go through its process, and at the end of that process, I am hopeful and expecting that he'll be extradited."

Nikulin was extradited just days later, even as the decision looked like it would be reviewed.

Zeman has since made very bizarre comments criticizing Ryan for his involvement.

> Zeman said he had a different view of the Nikulin case than Justice Minister Robert Pelikan (ANO), who had given consent to the extradition of this Russian citizen to the USA, but that he fully respected the minister's right to decide on this matter.
>
> Apart from the United States, Russia was seeking Nikulin's extradition, too, based on a suspected online theft.
>
> "When Donald Trump was elected American president, (U.S. House of Representatives Speaker Paul) Ryan wore a black tie. The same Mr Ryan arrived in the Czech Republic (last week). He publicly stated that he had arrived basically in order to get Mr Nikulin to the United States, in which he succeeded. Well, one of the versions is that Mr Nikulin may in some way serve as a tool of the internal American political fight – to which the black tie served as well," Zeman said.
>
> "I do not consider this a very good solution if Czechs were to meddle in the American political situation," Zeman added.
>
> Ryan, who appreciated the Czech government for the extradition of Nikulin, did not meet Zeman during his recent visit to Prague without citing the reasons.

It may be that Ryan was doing the bidding of Trump. Or, more likely, Ryan may have made the move in what appears to be fairly unified NATO response to the attempted Sergei Skripal assassination.

Nikulin's Russian-provided lawyer makes it clear they will negotiate

That said, I find it very interesting that Nikulin's lawyer, whom the Russians asked to get involved, is explicitly already talking about a plea deal.

> The legal team for Yevgeniy Nikulin, the Russian hacker accused of stealing data from LinkedIn and other American tech firms, will explore a plea deal with the U.S. government, according to Nikulin's lawyer, Arkady Bukh.
>
> "The likelihood of a trial is not very high," Bukh said. The U.S. District Court for the Northern District of California, where Nikulin's trial would occur, "has over a 99 percent conviction rate. We are not throwing clients under the bus," Bukh said.
>
> [snip]
>
> Bukh was first contacted by the Russian consulate and asked to help on the case. He was approved on Wednesday to act as a lawyer for Nikulin by the court. Although Bukh has been in regular and sustained contact with both Nikulin's family and the Russian consulate, he had yet to speak with his client as of Wednesday night.
>
> The Russian consulate has expressed concerns about Nikulin's mental condition, and Bukh said he "appears to be depressed."

Perhaps Bukh is taking this route because the Feds have Nikulin dead to rights and a plea is the most logical approach. Perhaps Russia has

learned its lesson from Roman Seleznev, the son of a prominent Duma member, who has been shipped around to different jurisdictions to have additional onerous sentences added to his prison term; I'm fairly certain there are other sealed indictments against Nikulin besides the one he was charged under that DOJ could use similarly.

Or perhaps Russia has reason to want to bury any public airing of evidence regarding what Nikulin has done or could be said to have done.

How Nikulin might be involved in the 2016 operation

I've long suggested that Nikulin may have had a facilitating role in the 2016 operation. That's because credentials from his LinkedIn hack were publicly sold for a ridiculously small amount just before May 18, 2016, rather inexplicably making them available outside the tight-knit group of Russians who had been using the stolen credentials up to that point.

Almost all of the people whose email boxes were sent to Wikileaks were affected by the LinkedIn (and/or MySpace) breach, meaning passwords and emails they had used became publicly available in the middle of the Russian operation. And those emails were exfiltrated in the days immediately following, probably May 19-25, the public release of those credentials.

In other words, it is possible that stolen credentials, and not GRU hacks, obtained the emails that were shared with WikiLeaks.

None of that is to say that Russia didn't steal the emails shared with Wikileaks or arrange that handoff.

Rather, it's to say that there is a counter-narrative that would provide convenient plausible deniability to both the Russians and Wikileaks that may or may not *actually* be how

those emails were obtained, but also may be all wrapped up ready to offer as a narrative to undercut the claim that GRU itself handed off the emails.

Note, too, how that timing coincides with the public claims Konstantin Kozlovsky made last year, which I laid out here.

> April 28, 2015: FSB accesses Lurk servers with Kaspersky's help.
>
> May 18, 2016: LinkedIn credentials allegedly stolen by Yevgeniy Nikulin made widely available.
>
> May 18, 2016: Kozlovsky arrest.
>
> May 19-25, 2016: DNC emails shared with WikiLeaks likely exfiltrated.
>
> October 5, 2016: Yevgeniy Nikulin arrest in Prague.
>
> October 20, 2016: Nikulin indictment.
>
> November 1, 2016: Date of Kozlovsky confession.
>
> December 5, 2016: Arrest, for treason, of FSB officers Dmitry Dokuchaev and Sergey Mikhailov.
>
> February 28, 2017: Indictment (under seal) of FSB officers, including Dmitry Dokuchaev, Alexey Belan, and Karim Bartov for Yahoo hack.
>
> March 15, 2017: Yahoo indictment unsealed.
>
> August 14, 2017: Kozlovsky posts November 1 confession of hacking DNC on Facebook.
>
> November 28, 2017: Karim Baratov (co-defendant of FSB handlers) plea agreement.
>
> December 2, 2017: Kozlovsky's claims posted on his Facebook page.

> March 30, 2018: Extradition of Nikulin.
>
> April 2, 2018: Report that Dokuchaev accepted a plea deal.
>
> April 17, 2018: Scheduled court appearance for Nikulin.

With each new hacker delivered into US custody, something happens in Russia that may provide an alternate narrative.

And consider that in the wake of Nikulin's extradition, Dmitry Dokuchaev and another of the people accused of treason in Russia have made a partial confession that will, like any Nikulin plea, serve to bury much of the claimed evidence against them.

> Two of the four suspects in a Russian treason case, including a former agent in the FSB's Information Security Center, have reportedly signed plea bargains where they confess to transferring data to foreign intelligence agencies. Three sources have confirmed to the magazine *RBC* that former FSB agent Dmitry Dokuchaev and entrepreneur Georgy Fomchenkov reached deals with prosecutors.
>
> One of *RBC*'s sources says the two suspects claim to have shared information with foreign intelligence agencies "informally," denying that there was anything criminal about the exchange. Dokuchaev and Fomchenkov say they were only trying to help punish cyber-criminals operating outside Russia and therefore outside their jurisdiction. Lawyers for the two suspects refused to comment on the story.
>
> As a result of the plea bargains, the two men's trials will be fast-tracked in a special procedure where the evidence collected against them isn't reviewed.

> Dokuchaev and Fomchenkov will also face lighter sentences – no more than two-thirds of Russia's maximum 20-year sentence for treason, says one of *RBC*'s sources.
>
> The other two suspects in the treason case, former FSB Information Security Center agent Sergey Mikhailov and former Kaspersky Lab computer incidents investigations head Ruslan Stoyanov, have reportedly turned down plea bargains, insisting on their innocence.

All of which is to say that Nikulin offers at least a plausible counter-explanation for the DNC hack-and-leak, one that might shift blame for the operation to non-state actors rather than GRU, which is something Vladimir Putin has been doing since Nikulin's extradition first became likely, even if he has changed his mind about whether such non-state Russians will be celebrated or demonized upon their roll-out.

Rolling out plea deals here and in Russia may be an effort to try to sell that counter-narrative, before Robert Mueller rolls out whatever he will about the hack-and-leak in coming days.

Update: A reader notes correctly that all the dossier's reporting on Cohen, especially that describing a meeting in Prague, post-dates the Nikulin arrest. See this post for more on the timing of the Cohen reporting, piggy-backing off of PiNC's analysis.