THE TRUMP HACK COULD EXTEND FAR BEYOND A HACK-AND-LEAK

When news first broke that Donald Trump's campaign says it has been hacked, I started drafting a post on applying the lessons of past ratfucks.

The alleged hack was first reported by Politico, which says some person using an AOL account reached out and shared documents, including the vetting materials pertaining to JD Vance and Marco Rubio.

> On July 22, POLITICO began receiving emails from an anonymous account. Over the course of the past few weeks, the person — who used an AOL email account and identified themselves only as "Robert" — relayed what appeared to be internal communications from a senior Trump campaign official. A research dossier the campaign had apparently done on Trump's running mate, Ohio Sen. JD Vance, which was dated Feb. 23, was included in the documents. The documents are authentic, according to two people familiar with them and granted anonymity to describe internal communications. One of the people described the dossier as a preliminary version of Vance's vetting file.
>
> The research dossier was a 271-page document based on publicly available information about Vance's past record and statements, with some — such as his past criticisms of Trump — identified in the document as "POTENTIAL VULNERABILITIES." The person also sent part of a research document about Florida Sen. Marco Rubio, who was also a

> finalist for the vice presidential nomination.

Trump's bouncer-spox, Steven Cheung, claims the hack was done by Iran, citing a Microsoft report released Friday describing the compromise by Iran of the email account of a "former senior advisor," which the IRGC then used to attempt to compromise a current high-level official.

> Yet another Iranian group, this one connected with the Islamic Revolutionary Guard Corps, or IRGC, sent a spear phishing email in June to a high-ranking official on a presidential campaign from the compromised email account of a former senior advisor. The email contained a link that would direct traffic through a domain controlled by the group before routing to the website of the provided link. Within days of this activity, the same group unsuccessfully attempted to log into an account belonging to a former presidential candidate. We've since notified those targeted.

A pity for the Trump campaign that Cheung is a habitual liar, so we can't trust anything he says, and Politico's authentication appears to rely exclusively on word of mouth from those who have the documents, not digital authentication.

Still, it's distinctly possible. The FBI certainly seems to believe the IRGC is trying to assassinate Trump.

The lessons I was going to propose in my draft post were the following:

- Vice President Harris should eschew assigning her senior-most staff to exploiting these emails like Trump did in 2016.

- But only after Trump, Don Jr, and Mike Pompeo apologize for their enthusiastic use of hacked emails in 2016.
- The same 51 former spooks who warned that the Hunter Biden laptop had the earmarks of a foreign influence operation should write a similar letter here, emphasizing (as they did in their Hunter Biden letter) the import of resisting foreign efforts to influence a presidential election. Maybe Peter Strzok and Andy McCabe could join in. Chris Krebs, who already has weighed in validating the seriousness of the threat, but who was fired for telling the truth about the 2020 election, can join too. They should send it to Politico, which first reported this story, but CC Jim Jordan, who says even writing such a letter is an abuse of First Amendment protected free speech.
- Donald Trump must provide all the affected servers to the FBI, stat.

It's the last one that was going to be my punch line. Partly because of misleading (arguably inaccurate) Jim Comey testimony, and partly

because a wide swath of people had an incentive to do Russia's bidding, for eight years people, including many in Congress, have been suggesting that a hacking victim must give all the servers that were hacked to law enforcement — the actual servers, not forensic images — otherwise the FBI's investigation would be suspect.

They were wrong on several counts. But they were loud and insistent.

Fine. Based on that precedent, Trump must hand over his campaign servers to the same FBI that has criminally investigated him, including his campaign finance shenanigans, immediately.

That's what I was going to write when Politico's Alex Isenstadt, who is not a journalist competent to report a hack-and-leak story, was the only one who had written this up.

But then WaPo wrote it up, with Trump-whisperer Josh Dawsey and horserace journo Isaac Arnsdorf bylined, but also Ellen Nakashima and Shane Harris, the latter two of whom are exceptional reporters for a story about hacking.

That story had two additional details that made me rethink the potential impact of this. First, it revealed that *Trump didn't tell the FBI about the hack*.

> People familiar with the matter said the campaign separately concluded earlier this summer its email system had been breached but did not disclose it publicly or to law enforcement. The people said some officials were told to take more protective measures on their email accounts. At the time, campaign officials communicated to others that they weren't sure who hacked the emails.

It's not even clear whether Trump got an outside contractor — and if so, if it was someone more competent than Rudy Giuliani, whom Trump once pitched as a cybersecurity expert — to help clean up this mess. It took Crowdstrike and the

DNC over a month to attribute the Russian hack, but they never fully cleaned it up. And persistent attacks continued through the election. That is, even with a respected outside contractor, the Democrats were wasting energy on whack-a-mole defense efforts for the remainder of the election.

Against that background, WaPo's description of *what* the persona shared becomes more alarming.

> On Thursday, The Washington Post was also sent a 271-page document about Vance from a sender who called himself Robert and used an AOL email account. Dated Feb. 23 and labeled "privileged & confidential," the document highlighted potential political vulnerabilities for the first-term senator. Two people familiar with the document confirmed it was authentic and **was commissioned by the campaign from Brand Woodward**, a law firm that represents a number of prominent Trump advisers in investigations by state and federal authorities.
>
> The document drew from publicly available information, including past news reports and interviews with the senator. The campaign commissioned several reports of other candidates, too, the advisers said.
>
> The sender would not speak on the telephone with a Post reporter but indicated they had access to additional information, **including internal campaign emails and documents related to Trump's court cases**. [my emphasis]

First, Brand Woodward did the campaign's vetting.

Stan Woodward represents, along with others, Walt Nauta, Kash Patel, and Peter Navarro in various Trump-related criminal investigations,

as well as some seditionists. He's a great fit for Trump insofar as he's good at generating outrage over manufactured slights — though in front of regular judges, those complaints usually collapse. Multiple filings in the documents case suggest that Woodward has a tenuous relationship with digital technology.

The role of Stan Brand, Woodward's partner, has been assiduously hidden, except insofar as he has made claims about cases to the press on-the-record without disclosing the tie to Woodward.

Now, WaPo has confirmed that the Microsoft description — of a former advisor pwned and using that person's email account, an attempt to hack "a high-official" still on the campaign — pertained to the Trump campaign. Given that description, there's no reason to believe that Woodward or Brand were affected.

But there's nevertheless a problem with hiring Brand Woodward to do your candidate vetting. To be clear: Brand is absolutely qualified to do that kind of thing. He's got a long record of doing so in congress. But even Trump appears to have concerns about major issues the vetting process missed, to say nothing of his donors.

> Over the past two weeks, Mr. Trump has fielded complaints from donors about his running mate, JD Vance, as news coverage exploring Mr. Vance's past statements unearthed — and then exhaustively critiqued — remarks including a lament that America was run by "childless cat ladies."
>
> Mr. Trump dismissed out of hand donors' suggestions that he replace Mr. Vance on the ticket. But Mr. Trump privately asked his advisers whether they had known about Mr. Vance's comments about childless women before Mr. Trump chose him.

There were *better* choices to vet candidates, but if Trump wants to let a thin team vet the surly

troll he picked to be his running mate, that's his own business.

My alarm about the news that Brand Woodward starts, however, by the way that the Trump campaign has muddled various functions, criminal and civil defense with campaign finance and, now, candidate vetting. It creates a legal morass, one that — if Trump loses this election — could lead to more legal trouble down the road.

Maybe that's why Trump didn't call the FBI.

But it also means that some people — most notably, Susie Wiles and Boris Epshteyn, along with Woodward and Brand — are playing multiple functions. Wiles is the one who decides who gets their criminal defense bills paid, she's also the one who decides how to spend campaign cash, and she was a big backer of the JD pick.

When people play overlapping functions like that, it means that a hack targeted at them for one function — say, candidate vetting — may strike a gold mine of documents pertaining to another function — say, criminal defense.

WaPo's reference to "documents related to Trump's court cases" — Politico quoted the persona offering a "variety of documents from [Trump's] legal and court documents to internal campaign discussions" — may ultimately pertain exclusively to Trump's electoral court cases. If it does, those could be some of the most newsworthy out there, since Trump's electoral court cases pose a direct threat to democracy.

But what if they don't? What if these documents pertain to what those overlap people — people like Wiles or Epshteyn, and they're only two of the most obvious —know about Trump's criminal cases? What if they pertain to claims that witnesses have made to the FBI about where documents got moved or what was included in them? What if they pertain to the actual documents Trump stole, starting with the US strategic plan against Iran that Trump shared with Mark Meadows' ghost writers?

Trump has not firewalled his campaign from a criminal case involving the most sensitive documents of the US government, meaning a well-executed hack targeted at his campaign may turn into an intelligence bonanza.

If Iran plans to make things difficult for Trump, the problems may extend well beyond what documents get leaked. As they did in 2016, this could mean that Trump wastes resources having to serially defend against hacking attempts via a range of different platforms. It could mean that Iran does what Russia did, hack key strategic models to optimize other kinds of fuckery later in the election. Because — unlike Russia — Iran is actively trying to kill Trump, not just defeat him, hacked documents may also facilitate efforts like those charged against Asif Merchant, manufacturing fake protests to create distractions to facilitate an assassination attempt.

The question of how to approach this news, if it is further confirmed, goes well beyond the question of whether to publish the documents allegedly stolen by Iran. In significant part *because* Trump refuses to maintain boundaries between his political life and his criminal life, hacks from Iran could create real damage to the United States beyond what they do to Trump's campaign.

So by all means, let's pause for a moment of schadenfreude. Let's review all the things Trump said and did in 2016 and 2020 (including with the Hunter Biden laptop) that invite his opponents to fully exploit stolen documents this time.

But as you do that, consider that this ratfuck may be far more dangerous to the US than those targeting Hillary and Hunter.