

# NSA IS PROBABLY WITHHOLDING DETAILS OF THE ALLEGED BURISMA HACK FROM CONGRESS

Over the weekend, Adam Schiff and other impeachment managers started alleging that the NSA is withholding information about Ukraine from the Intelligence Committees and impeachment team.

“And I’ll say something even more concerning to me, and that is the intelligence community is beginning to withhold documents from Congress on the issue of Ukraine,” Schiff said. “The NSA, in particular, is withholding what are potentially relevant documents to our oversight responsibilities on Ukraine, but also withholding documents potentially relevant that the senators might want to see during the trial.”

Schiff added: “There are signs that the CIA may be on the same tragic course. We are counting on the intelligence community not only to speak truth to power, but to resist pressure from the administration to withhold information from Congress because the administration fears that they incriminate them.”

An Intelligence Committee official later said, “Both the NSA and CIA initially pledged cooperation, and it appears now that the White House has interceded before production of documents could begin.”

Schiff had dropped the claim, at times, in his presentation to the Senate and to the press.

But in his stem-winding close last night, he mentioned the alleged Burisma hack in a way that strongly suggests that's what NSA is withholding.

Now we just saw last week a report that Russia tried to hack, or maybe did hack, Burisma. Okay. I don't know if they got in. I'm trying to find out. My colleagues on the Intel Committee, House and Senate, we're trying to find out, did the Russians get in? What are the Russian plans and intentions? Well, let's say they got in. And let's say they start dumping documents to interfere in the next election. Let's say they start dumping some real things they hacked from Burisma, let's say they start dumping some fake things they didn't hack from Burisma, but they want you to believe they did. Let's say they start blatantly interfering in our election again, to help Donald Trump. Can you have the least bit of confidence that Donald Trump will stand up to them and protect the national interest over his own personal interest? You know you can't.

Schiff's speech was a planned show-stopper, climax, thus far, of the impeachment trial. It is highly unlikely Schiff included this mention, with the detail that he and both the Intelligence Committees are trying to figure out whether Burisma really got hacked, without very good reason.

But it also goes to the power of information war.

When NYT first reported that GRU had hacked Burisma, I had two thoughts.

The hackers fooled some of them into handing over their login credentials, and managed to get inside one of Burisma's servers, Area 1 said.

"The attacks were successful," said Oren Falkowitz, a co-founder of Area 1, who previously served at the National Security Agency. Mr. Falkowitz's firm maintains a network of sensors on web servers around the globe – many known to be used by state-sponsored hackers – which gives the firm a front-row seat to phishing attacks, and allows them to block attacks on their customers.

"The timing of the Russian campaign mirrors the G.R.U. hacks we saw in 2016 against the D.N.C. and John Podesta," the Clinton campaign chairman, Mr. Falkowitz said. "Once again, they are stealing email credentials, in what we can only assume is a repeat of Russian interference in the last election."

[snip]

To steal employees' credentials, the G.R.U. hackers directed Burisma to their fake login pages. Area 1 was able to trace the look-alike sites through a combination of internet service providers frequently used by G.R.U.'s hackers, rare web traffic patterns, and techniques that have been used in previous attacks against a slew of other victims, including the 2016 hack of the D.N.C. and a more recent Russian hack of the World Anti-Doping Agency.

"The Burisma hack is a cookie-cutter G.R.U. campaign," Mr. Falkowitz said. "Russian hackers, as sophisticated as they are, also tend to be lazy. They use what works. And in this, they were successful."

First, this attribution is not (yet) as strong as even the first attribution that GRU had hacked the DNC, to say nothing of the 30 non-government sources for that attribution since laid out in the GRU indictment and the Mueller

Report. There's good reason to remain cautious about this attribution until we get more than one not very well established contractor attributing the hack.

But to some degree, it doesn't matter whether GRU hacked Burisma and whether they took documents with plans to leak them during the election. Indeed, disinformation may explain why this was an easily identifiable hack, whether done by GRU or someone else. Because the news that someone appearing to be GRU targeted Burisma in early November – when it was clear Trump would be impeached for extorting Volodymyr Zelensky to get dirt on Burisma – serves a clear purpose. It adds evidence that Trump is owned by Russia and, after the Senate doesn't vote to remove him, will demonstrate that Republicans don't much give a damn that he is owned by Russia.

To be clear: There's abundant evidence that Russia does have leverage over Trump, and more is likely to be forthcoming.

But that's far more valuable, for Russia, if that's public and if the Republicans in the Senate sanction it.

And that may explain why NSA is withholding the information, if indeed that's what they're withholding. In the same way that the FBI went to great lengths to withhold a letter they believed to be disinformation suggesting that Loretta Lynch would fix the Hillary investigation, information that appears to add to the already abundant case that Russia is in the tank for Trump. Given the stakes, that doesn't justify it. But at this point, GRU wouldn't need to hack Burisma for any point – the hack itself, in the middle of the impeachment investigation, is enough to lay a marker on Donald J. Trump.

He belongs to the GRU, the hack says, whether or not he does anything affirmatively to confirm that claim. But if the NSA is withholding that detail, it would seem to confirm the point.