THE RUSSIANS ARE COMING! THE RUSSIANS ARE — OOPS! NO RUSSIANS!

In my piece on Sunday on the package of sanctions the government released last week, I noted the likelihood the Joint Analysis Report would result in false positives.

> But several of the reports also include some version of this conclusion from Lee: "the indicators are not very descriptive and will have a high rate of false positives for defenders that use them."
>
> That is, we may see more of what we saw Friday, when a Vermont utility did as instructed with the report — searched for the indicators included in the report — reported a positive hit, only to have anonymous sources immediately blow it up to mean Russia had hacked our grid. That find might turn out to be a Russian probe, or it might not; there's little doubt that Russia can hack our electrical system. But what it did do is feed a panic.

Sure enough, that's what Friday's alarmist WaPo story turned out to be. Another WaPo story last night revealed that there's no evidence Russian

government hackers were in Burlington Electric — indeed, it sounds like what the utility might have found was one of the many Tor or other innocuous IP addresses included in the report.

> As federal officials investigate suspicious Internet activity found last week on a Vermont utility computer, they are finding evidence that the incident is not linked to any Russian government effort to target or hack the utility, according to experts and officials close to the investigation.
>
> An employee at Burlington Electric Department was checking his Yahoo email account Friday and triggered an alert indicating that his computer had connected to a suspicious IP address associated by authorities with the Russian hacking operation that infiltrated the Democratic Party. Officials told the company that traffic with this particular address is found elsewhere in the country and is not unique to Burlington Electric, suggesting the company wasn't being targeted by the Russians. Indeed, officials say it is possible that the traffic is benign, since this particular IP address is not always connected to malicious activity.

As it happens, after the government took custody of they laptop, they found *other* malware, not associated with Russians, on the laptop, but which wasn't found as a result of last week's report and scan.

> In the course of their investigation, though, they have found on the device a package of software tools commonly used by online criminals to deliver malware. The package, known as Neutrino, does not appear to be connected with Grizzly Steppe, which U.S. officials have

> identified as the Russian hacking operation. The FBI, which declined to comment, is continuing to investigate how the malware got onto the laptop.

But ultimately, Friday night's scare, with comments from half of Vermont's public officials, was about an IP address that has no definitive tie to the Russians.

And that wasn't the only false positive arising from this report. A Dutch paper did a story accusing a key Dutch privacy person (Bits of Freedom is sort of like EFF) of running a Tor node used by the Russians, as if Tor node operators sign off on the traffic that transits their nodes.

Remember: one of the primary claimed goals of Russia's hacking is to make Americans lose trust in our government. Because of the way this report and subsequent reporting was rolled out (and leaked to a White House beat reporter), both security professionals and the general public will lose confidence not just in the government's ability to respond to hacks, but also in the government's report claiming the Russians were behind the hack. Not to mention, the alarmist report has led the paper that pushed the PropOrNot bullshit to make this kind of claim, blaming sources but not their own reporting.

> Authorities also were leaking information about the utility without having all the facts and before law enforcement officials were able to investigate further.

Remember: WaPo first published the story before getting any comment from Burlington Electric.

The government appears to be doing Vlad Putin's work for him, damaging its own credibility in its efforts to combat his efforts to damage its credibility.