ABOUT THAT RUSSIAN HACKER STORY

This story is going viral on social media. The CNN article, dated October 12, describes a compromise of a FL contractor they don't situate in time.

> Federal investigators believe Russian hackers were behind cyberattacks on a contractor for Florida's election system that may have exposed the personal data of Florida voters, according to US officials briefed on the probe.
>
> *The hack of the Florida contractor comes on the heels of hacks in Illinois, in which personal data of tens of thousands of voters may have been stolen, and one in Arizona, in which investigators now believe the data of voters was likely exposed.*

Later in the article, CNN makes it clear this is the same hack as described in this earlier ABC reporting, which expands on a story from several days earlier. ABC's reporting doesn't date the compromise either. Rather, it explains that FL was one of four states in which hackers had succeeded in compromising data, whereas hackers had scanned voting related systems — tried to hack systems — in half the states.

> As ABC News first reported Thursday, hackers have recently tried to infiltrate voter registration systems in

> nearly half of the states across the country —- a significantly larger cyber-assault than U.S. officials have been willing to concede.
>
> And while officials have publicly admitted Illinois and Arizona had their systems compromised, officials have yet to acknowledge that information related to at least two other states' voters has also been exposed.
>
> Hackers working on behalf of the Russian government are suspected in the onslaught against election-related systems, according to sources with knowledge of the matter.

And ABC's source at least claimed that all hackers did was copy voter data.

> The voter information was exposed after cyber-operatives gained entry to at least one computer associated with a private company hired to administer voter information, the sources said.
>
> A simple "phishing" scheme —- with a malicious link or attachment sent in an email —- is likely how it all started, one source said.
>
> "The attack was successful only in the sense that they gained access to the database, but they didn't manipulate any of the voter [information] in the database," the source said.

So, in spite of what people might think given the fact that the CNN is going viral *right now*, it doesn't refer to a hack in conjunction with the election. It refers to a hack that happened well over a month ago. It refers to a hack that — at least according to people who have an incentive to say so — resulted only in the theft of data, not its alteration.

Both CNN and ABC use language that suggests the

Russian government was behind this hack. Here's CNN:

> FBI investigators believe the the hacks and attempted intrusions of state election sites were carried out by hackers working for Russian intelligence.

And here's ABC:

> Hackers working on behalf of the Russian government are suspected in the onslaught against election-related systems, according to sources with knowledge of the matter.

But (as CNN points out) the October 7 joint DNI/DHS statement on Russian hacking doesn't attribute the voting rolls part to the Russian state.

> Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government.

An earlier DHS one explicitly attributes them to cybercriminals.

> (U//FOUO) DHS has no indication that adversaries or criminals are planning cyber operations against US election infrastructure that would change the outcome of the coming US election. Multiple checks and redundancies in US election infrastructure—including diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaign, and election officials to check, audit, and validate results—make it likely that cyber manipulation of US

> election systems intended to change the outcome of a national election would be detected.
>
> (U//FOUO) We judge cybercriminals and criminal hackers are likely to continue to target personally identifiable information (PII), such as that available in voter registration databases. We have no indication, however, that criminals are planning theft of voter information to disrupt or alter US computer-enabled election infrastructure.

There were known instances of identity thieves hacking voting rolls going back some time, so it is possible that's all this was about.

We learned recently that FBI Director Comey pointedly did not want to be included on the joint DNI/DHS statement, because it was too close to the election. So it's possible there was disagreement about that part of it (which might explain the FBI-sourced leak to CNN).

Also note, I believe the known hackers used different methods, including both SQL injection and phishing. If in response to the earlier ones, DHS did a review of voting systems and found a number of phishes using the same methods as GRU, that may explain why FBI would say it was Russian.

In any case, we don't know what happened, and at least public claims say the hackers didn't alter any data.

But the CNN story, at least, is not about something that just happened.

Update: Fixed some typos and clarity problems.