

MEDIA CRITICISM: THE PRESS NEEDS TO GET FAR MORE RIGOROUS ABOUT REPORTING ON CYBERSECURITY

Four days ago, NBC reported, as BREAKING news, that in an exclusive interview, Jeanette Manfra had confirmed that the voter rolls of 21 states were targeted in 2016.

*Russians
penetrated U.
S. voter
systems,
top U.S. offi-
cial says*

The U.S. official in charge of protecting American elections from hacking says the Russians successfully penetrated the voter registration rolls of several U.S. states prior to the 2016 presidential election.

In an exclusive interview with NBC News, Jeanette Manfra, the head of cybersecurity at the Department of Homeland Security, said she couldn't talk about classified information publicly, but in 2016, "We saw a targeting of 21 states and an exceptionally small number of them were actually successfully penetrated."

The headline stated and this video (which has been viewed *online* by 50,000 people) stated explicitly that 21 states were "penetrated."

I criticized all the breathless retweeting of

the report in a subtweet.



emptywheel
@emptywheel

Folks: When we learned that the Russians had penetrated IL and AZ's voter registration rolls, didn't we know that "Russians successfully penetrated voter registration rolls of several U.S. states prior to 2016 presidential election"?

10:02 PM - 7 Feb 2018

Today, DHS did more than subtweet the report and the irresponsible sharing of it. It released a scathing complaint, in Jeanette Manfra's (the woman NBC interviewed) name, about NBC's reporting, specifically complaining that NBC reported the number as "breaking" news.

Recent NBC reporting has misrepresented facts and confused the public with regard to Department of Homeland Security and state and local government efforts to combat election hacking. First off, let me be clear: we have no evidence – old or new – that any votes in the 2016 elections were manipulated by Russian hackers. NBC News continues to falsely report my recent comments on attempted election hacking – which clearly mirror my testimony before the Senate Intelligence Committee last summer – as some kind of "breaking news," incorrectly claiming a shift in the administration's position on cyber threats. As I said eight months ago, a number of states were the target of Russian government cyber actors seeking vulnerabilities and access to U.S. election infrastructure. In the majority of cases, only preparatory activity like scanning was observed, while in a small number of cases, actors were able to access the system but we have no evidence votes were changed or otherwise impacted.

NBC's irresponsible reporting, which is being roundly criticized elsewhere in

the media and by security experts alike, undermines the ability of the Department of Homeland Security, our partners at the Election Assistance Commission, and state and local officials across the nation to do our incredibly important jobs. While we'll continue our part to educate NBC and others on the threat, more importantly, the Department of Homeland Security and our state and local partners will continue our mission to secure the nation's election systems.

To our state and local partners in the election community: there's no question we're making real and meaningful progress together. States will do their part in how they responsibly manage and implement secure voting processes. For our part, we're going to continue to support with risk and vulnerability assessments, offer cyber hygiene scans, provide real-time threat intel feeds, issue security clearances to state officials, partner on incident response planning, and deliver cybersecurity training. The list goes on of how we're leaning forward and helping our partners in the election community. We will not stop, and will stand by our partners to protect our nation's election infrastructure and ensure that all Americans can have confidence in our democratic elections.

In response to my observation that NBC should never have presented it as "breaking" news and my subsequent suggestion that it'd be far more useful to educate people about what "compromise" can mean, Ken Dilanian got pissy, suggesting I don't do reporting.



KenDilanianNBC ✓

12:11

Replying to @emptywheel

Maybe you could take off your media critic hat, jump in the trenches and do some reporting of your own on this issue. In fact, if you come up with the classified list of states that were penetrated by Russian hackers, I'll happily retweet it. @Tom_Winter

When I retweeted the video above (h/t K), suggesting maybe Dilanian could educate viewers about what both “compromise” and “penetrate” mean, he responded “Or you could focus on your own reporting.”

Only, we don't need NBC to do that. We can go back to Manfra's testimony from June, where she distinguished between “compromise,” unsuccessful compromise,” and “scanning.”

One comprehensive intelligence report published by the Office of Intelligence and Analysis in early October, cataloged suspicious activity we observed on state government networks across the country. This initial look, largely based on suspected malicious tactics and infrastructure, helped inform a body of reporting directly related to election infrastructure. While not a definitive source in identifying individual activity attributed to Russian government cyber actors, it established that Internet-connected election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors. Although we've refined our understanding of individual targeted networks, supported by classified reporting, the scale and scope noted in that October 2016 report still generally characterizes our observations: a small number of networks were successfully compromised, there were a larger number of states where attempts to compromise networks were unsuccessful, and there were an even greater number of states

where only preparatory activity like scanning was observed.

Admittedly, we'd all be better served if Manfra had provided more detail about precisely what these terms mean.

But absent that, the press should be far more cautious reporting on various degrees of hacking, as most people don't understand the difference between a scan, a compromise, and damage from such compromise.

And lest Dilanian think I wrote this up just to document what a horse's ass he was in response to well-earned criticism, I should note I'm supposed to be working on this issue in conjunction with a fellowship I've got – it turns out I've got a meeting this week where this example will come in very handy, thus the value of documenting it.

The explanation for Russia's 2016 election-related hacking that everyone will agree on is that they did it to sow distrust in democracy. But shitty reporting on attempts to hack our democracy does that just as well.