

## The Biggest Threat to US Elections are Facebook and Google's Youtube -- NOT Russia!

by Steven Rosenfeld via jane - Alternet Sunday, Feb 11 2018, 6:45pm

international / prose / post

Silicon Valley algorithms while suppressing alternative news sites help spread conspiracy theories peddled by questionable American sources.

Americans who care about democracy and voting should stop jumping to conclusions about Russians hunkered down in Moscow [cyber-bunkers](#), and instead look at what's happening on these shores as shoddy journalists and Silicon Valley's content curators are doing Vladimir Putin's work for him.

Last week, a mini-drama played out in the world of American elections, Russian interference and vote-hacking conspiracies that was a microcosm of the same online dynamics that tilted and [force-fed](#) American voters [seven times](#) as much Hillary-hating propaganda on YouTube as comparable anti-Trump content.

This snapshot reveals that little has changed in the misinformation engines driving the attention economy. This is the frail state of American democracy today, where the most powerful content curators, opportunistic partisans, poorly informed journalists—and yes, overseas adversaries—are funneling and amplifying “divisive, sensational and conspiratorial” content, as one authoritative [report](#) put it, further undermining already shaky public confidence in voting.

“Russia probably realizes, despite what a lot of people in the progressive community and other communities probably think, it's really hard to change the outcome in a race; to change it [the count] to what they might want to occur,” said a former Justice Department lawyer who now advises state election officials. “That [theft] would require a lot of Americans engaged in an active conspiracy here on the ground; thousands of people.”

“But for less money and risk, they can get us to do their job for them,” he said. “They can get us to doubt our own election system; to doubt the machinery of American democracy. And they have been enormously successful in that. And I think the NBC piece [this week] is part and parcel of that. When you talk about, hysterically, risks that everyone has known about for nearly a year, and you don't talk about all the work that's been done since then, you don't interview a single election official, you're basically trying to put people into a state of hysteria about how their vote is not going to count. That's really damaging. That's going to undermine our democracy.”

### Misinformation Engines

Americans received more bad news about voting this week. But amid all the news—such as Secretary of State Rex Tillerson [saying](#) that Russia was already interfering in 2018's elections but giving no details—one sloppy report stood out and ignited a stream of copycat and increasingly conspiratorial posts amplified by the web's content-pushing algorithms. On Wednesday, NBC News aired an “exclusive” [interview](#) with Jeanette Manfra, the Department of Homeland Security cyber security head, who reported that Russia had not targeted, but “penetrated” state voter systems in 2016.

First, NBC didn't understand what she said. "NBC chose to interpret that statement to mean 'several states' were successfully penetrated. We are still only aware of one state voter registration system that was penetrated and that office made a public statement at the time," the National Association of Secretaries of State noted on its website. Moreover, Manfra said nothing new. She repeated her [testimony](#) to Senate Intelligence Committee from June 2017, even using the same words.

Nonetheless, journalists who don't know how voting works, nor what Russia did and didn't do in 2016's elections, went wild. They quickly said what's most alarming and factually unsupported: that Russia all but stole the vote for Trump, or offered slightly less hyperbolic variations of that conspiratorial theme.

Esquire's [piece](#) ominously opened, "We are inching ever closer to the revelation that the actual vote totals were hacked—some very smart people are already there, by the way—and, once that happens, I don't know where we go from there." The Huffington Post [began](#), "The Russian government successfully obtained access to U.S. voter registration databases in multiple states." Under Reddit's [reposting](#) of the NBC video was a discussion filled with gripes about how dysfunctional our elections are, all escalating and pointing to the conclusion that the system is rigged, surely hacked and democratic hopes are a mirage.

Esquire offered no proof that the 2016 vote totals were tampered with—because there is none. That's not what election officials and technical advisors have said. Huffington Post got it wrong because Russian hackers only got inside one state's voter registration system, not multiple states. And most of the gripes on Reddit were due to political parties running primaries and caucuses in anti-democratic ways, or elected partisans who twist the rules of voting to benefit their base.

## What Did Russia Do?

These misinformed reports raced around the internet aided by algorithms that target content for people using sites like YouTube, Facebook and Twitter. That dynamic, an accelerating spiral in which misinformation and fiction outruns and [outperforms reality](#), is what arch partisans—as well as Russia—tapped in 2016 to influence voters. Yes, Russia got inside Illinois' registration database—a non-competitive blue state in the presidential year. But its hackers didn't tamper in a way that impeded polling place voting. That's what Russia achieved on a technical level and what top federal and state officials are trying to prevent again.

Russia also achieved a propaganda coup undermining the public's faith in American elections, which fits Putin's longstanding scorn for western democracy. But pointing the finger of blame at Russia for other 2016 snafus hasn't panned out. In North Carolina, some election integrity activists thought the scrambled poll books in Durham County were due to Russian interference. That suspicion came from the fact that the Florida-based contractor programming the voting machines had been identified as a target of another Russian phishing scheme that summer. Yet a deep post-mortem found another explanation: someone failed to delete poll book data from that spring's primary before setting up the machinery for November's vote. That mistake, in less than a half-dozen precincts, in turn, incorrectly told poll workers that people had already voted.

The problem there wasn't Russia, but a voting system where too many key features are privatized and managed by contractors protecting those trade secrets: the black box software running voting systems.

But back to the bigger picture. Nobody has found any proof that Russia accessed the separate computing systems that tallied 2016 votes, numerous consultants for state election officials and

federal authorities have repeatedly told AlterNet. Yet in 2018 we are living in a world where the spread of misinformation reigns, whether it is coming from media seeking greater audiences and ad revenues because suspense and conspiracy sells, or whether it's amplified by Silicon Valley's giant content curators that have programmed their algorithms to elevate "edgy and hateful content [because it] is engaging," as an authoritative investigative [report](#) in the Guardian put it.

What's clear is who and what is on the losing end of this escalating dynamic: any citizen who believes in the hope of democratic institutions like elections, despite their numerous flaws, from clumsy bureaucratic injuries to partisan betrayals.

Needless to say, there was other bad voting news this week; news that should have been given top billing by all these writers promoting the fable that Russia could have stolen 2016 for Trump and is back at it in 2018.

On Thursday, the Brennan Center for Justice at New York University Law School released a [report](#) declaring America's electronic voting machinery is "crumbling." The report red-flagged 41 states for systems that are more than a decade old, which is beyond the reliable lifespan of most computers, making "our elections more vulnerable to breakdown and malfunction, but to hacking as well." The Center issued a similar <https://www.brennancenter.org/publication/americas-voting-machines-risk> warning in 2015, calling on Congress to allocate several hundred million dollars to update the machinery. But that didn't happen then and it has not happened since, including in the two-year budget passed this week by Congress.

### What Really Matters Now?

In today's world, beyond raising awareness about the dark side of the attention economy, little is being done to substantively counter the reality that propaganda and paranoia are outrunning the facts, reality checks and better, more nuanced, information. Silicon Valley giants like Facebook and Youtube might publicly decry the use of their platforms to spread propaganda and fake news, but they are not changing their advertising systems that micro-target and deliver that content and reap them billions every quarter. Meanwhile, shoddy reporting that uses conspiracy theories to generate viewer traffic isn't helping.

Whether incomplete reporting (Tillerson's warning) or distortions presenting nothing new (NBC), or paranoid speculation built on those vapors (Esquire), election officials contacted by AlterNet say these kinds of narratives are eclipsing the steps now being taken to make voting in 2018 more secure and to better audit vote counts. But those granular steps won't matter if the public doesn't believe the results and is quicker to trust what flies around cyberspace at the speed of light.

What's been happening, and what people may start hearing about in coming weeks as 2018's first primary elections approach in March, is the result of unprecedented cooperation between the Department of Homeland Security and states to protect voting from cyber attacks. What Tillerson was apparently referring to when he said Russia is already trying to interfere in 2018's elections, was government voting systems—like computers across federal and state governments—are constantly being probed and targeted by overseas adversaries. That may be escalating, but it's not a new trend according to a state election director contacted by AlterNet.

Beyond this new federal-state cooperation, which was launched by the Obama administration, the federal Election Assistance Commission (EAC) will soon issue new voluntary voting system guidelines, which set higher standards for cyber security and audits to make sure votes are accurately counted. While these standards are voluntary, most states follow some or all of them, and

the private sector voting machine vendors typically adopt all of them.

Meanwhile, a handful of states, like Colorado and Rhode Island, are implementing better post-election audits. Other states are moving away from paperless voting, which Virginia did a few years ago. Louisiana is looking at this, dependent on funding, and so is Georgia, in a pilot project. Some of the pressure to do so—echoing what election integrity activists have long argued—is that the Election Assistance Commission push for better audits means using ink-marked paper ballots.

But back to 2018's elections and Russia. Unlike years past, better security and audits are the predominant focus for top election officials, who next weekend meet in Washington, D.C. The agendas for the National Association of Secretaries of State and National Association of State Election Directors both reflect this priority.

While it remains to be seen how effective these steps will be, it's a fact that it would be a colossal task to hack the statewide vote totals in a state like Michigan, with more than 1,600 different local and county election jurisdictions, each with separate voting systems, compared to targeting swing voters in swing counties on social media for edgy campaign messaging. (In Wisconsin there are 1,852 election jurisdictions; these are the two states that had the closest Clinton-Trump margins in 2016.)

In 2016, Russia's biggest impact was through propaganda, spreading messaging that pushed American voters' hot buttons, not tinkering with the machinery. That's why this week's microcosm, in which election hacking conspiracies eclipsed real news was noteworthy. It is a mirror of what's happening in our political and media culture, and points to the shape of things to come. In a year when midterm elections are poised to rebalance political power in America, undermining confidence in voting is the fastest lane to political chaos and unrest for Republicans to reject those results.

The stakes, as the ex-DOJ attorney said, "is people start doubting our own election system and they do not participate anymore. And it's what the election officials right now are fighting so hard against. They are working so hard to get the message out that they are on the job. They are working harder than ever. They are coordinating with the feds. They are trying to get the funding they need. So they can make sure that all future elections, even if the threat increases, that they can address it."

That's why this week's obsessive, incompetent reporting on Russian hacking—and the way it was amplified and spread online by Silicon Valley algorithms—presents real dangers to America's already imperfect democracy and system of voting and elections.

"We're doing Russia's work for them," the attorney said. "I don't think NBC is working for Putin. But because it's easy clickbait to say Russia's penetrating our election systems, even though this is literally the same language that [DHS cyber security director] Jeanette [Manfra] used for her testimony back in June. There's no one happier right now than Vladimir sitting on his throne in Moscow. This is exactly what he was hoping for. It's working."

Copyright applies.

<https://tinyurl.com/yd7pjawd>

