**Headline:** Why the Latest Cyber Attacks Were Disinformation, Not Voting System Breaches

**Teaser:** After murky high-profile media coverage, details emerge that question whether Iran was even involved.

By Steven Rosenfeld

**Author Bio:** Steven Rosenfeld is the editor and chief correspondent of [Voting Booth](https://votingbooth.media/), a [project](https://independentmediainstitute.org/voting-booth/) of the Independent Media Institute. He has reported for National Public Radio, Marketplace, and Christian Science Monitor Radio, as well as a wide range of progressive publications including Salon, AlterNet, the American Prospect, and many others.

**Source:** Independent Media Institute

**Credit Line:** *This article was produced by* [*Voting Booth*](https://votingbooth.media/)*, a* [*project*](https://independentmediainstitute.org/voting-booth/) *of the Independent Media Institute.*

**Tags:** Presidential Elections, Cybersecurity, Tech, Election Regulation, Voting Rights, North America/United States of America, Media, News, Politics, Trump, Time-Sensitive, Middle East/Iran, Europe/Russia, Intelligence Agencies

**[Article Body:]**

Two weeks before Election Day, cybersecurity threats and related disinformation originating overseas and targeting the 2020 election briefly were [front-page news](https://www.nytimes.com/2020/10/21/us/politics/iran-russia-election-interference.html).

Threatening emails to voters supporting Democrats were purportedly sent by the Proud Boys, a pro-Trump white nationalist group. State voter registration databases in Alaska and Florida were purportedly breached, and videos containing non-public voter information were posted online. As federal agencies blamed [Iran](https://www.ic3.gov/Media/News/2020/201022-2.pdf) and [Russia](https://www.ic3.gov/Media/News/2020/201022-1.pdf), an anxious electorate faced more worries.

“Sad but true, bad actors continue their attempts to undermine confidence in the election, now w/ a misleading video,” [tweeted](https://twitter.com/CISAKrebs/status/1319024445193920512) Chris Krebs, Cybersecurity and Infrastructure Security Agency (CISA) director, in one “Rumor Control” post on October 21. “Stay calm and vote on.”

The incidents—which were described, deconstructed, and debunked in non-technical terms in a Stanford Internet Observatory [report](https://www.eipartnership.net/rapid-response/foreign-election-interference-announcement) issued two days later—came in the same week that the U.S. [passed](https://electproject.github.io/Early-Vote-2020G/index.html) the 50 million mark for ballots already cast. The attacks may have been headline news, but they did not dent record turnout. Their false claims were swiftly outed and then drowned out by domestic noisemakers.

“Of course when it comes to spreading false information, the Russians have plenty of help from the President and his media allies,” [wrote](https://deepstateblog.org/2020/10/22/russian-intelligence-agencies-target-the-u-s-vote-abetted-by-trump/) longtime journalist Nina Burleigh on [Deep State blog](https://deepstateblog.org/), which monitors the world’s intelligence agencies, launching its series on foreign interference in the 2020 election.

Nonetheless, top federal officials who are allies of the president said the alleged Proud Boy emails and purloined voter registration data were [concrete evidence](https://www.nytimes.com/2020/10/21/us/politics/iran-russia-election-interference.html) of Russian and Iranian attempts to influence the 2020 election in its final weeks. But as news reports were filled with murky accusations, the Stanford [researchers](https://cyber.fsi.stanford.edu/io/content/io-teaching)—who include some of Silicon Valley’s foremost cybersecurity experts—concluded that no election data or computer systems had been breached. Instead, the propagandists—and the researchers found [no trace](https://www.eipartnership.net/rapid-response/foreign-election-interference-announcement) of Iranian involvement—fabricated content to fuel the impression that the 2020 nationwide election cannot be trusted.

“This series of events represents an active measures campaign intended to create the perception of a massive vulnerability in the U.S. election system that does not exist, and possibly to drive tension in the United States through the invocation of a well-known hate group,” the [report’s](https://www.eipartnership.net/rapid-response/foreign-election-interference-announcement) summation began. “Every conclusion that the creators of these emails and video wanted Americans to leave with are false:

* These intimidating emails were not sent by the Proud Boys
* Voting continues to be private, safe and secure, and there is no mechanism by which an outside actor can determine the vote of an individual and later threaten them
* The video does not portray a SQL injection attack against the Alaskan or Floridian voter registration systems
* There is no widespread conspiracy to change election outcomes via the FWAB [overseas and military absentee ballot] system
* Such a conspiracy could not succeed”

Another part of the analysis said, “We cannot provide independent attribution to the Islamic Republic of Iran,” which contradicted claims made by federal agencies.

**Election Vulnerabilities**

The emergence of foreign-based [threats](https://us-cert.cisa.gov/ncas/alerts/aa20-296a) that triggered high-profile news coverage but apparently had little impact on election infrastructure did not escape notice.

“[I]s this all they’ve got?” [wrote](https://electionlawblog.org/?p=117282) ElectionLawBlog founder Rick Hasen. “Why aren’t the Russians doing a better job interfering in the 2020 elections to benefit Trump?”

“The people behind this campaign were effective, however, in drawing attention to themselves and to their capability to create disinformation,” Stanford’s [report](https://www.eipartnership.net/rapid-response/foreign-election-interference-announcement) said. “The rapid reaction of government and civil society to these incidents has blunted the capability of these actors to spread their false claims. Our hope is, now that the video and emails have been thoroughly debunked, that media coverage of this disinformation is measured and that future attempts to imply hacking of the voting system are not given unearned amplification or credence.”

What was notable about the Stanford Internet Observatory [report](https://www.eipartnership.net/rapid-response/foreign-election-interference-announcement) was that its tone was neither alarmist nor dismissive. It was a sober assessment that threats, foreign and domestic, to disrupt the legitimacy of the 2020 election do exist. But, thus far, the foreign-based threats have not overwhelmed the system.

**What Was Faked?**

The voter data in the alleged attacks—such as partial Social Security numbers of Alaska voters—might not have come from hacking into a state voter database, as an online video claimed, for example. It could have come from stolen credit bureau data marketed on the dark web, the Stanford analysts [said](https://www.eipartnership.net/rapid-response/foreign-election-interference-announcement). What was of more concern, however, was that someone took the time to fashion that data into a falsified claim that voting infrastructure was easily breached.

“Releasing voter information and claiming it was hacked, as the newly-released video does, is not a new tactic,” the analysts said. “[Early last month](https://www.cyberscoop.com/russia-hack-michigan-voter-data-kommersant/), for example, claims spread by Russian media outlet Kommersant reported that Michigan’s voter data was posted on a Russian hacking forum. [EIP [Election Integrity Partnership] researchers verified](https://twitter.com/jackhcable/status/1300805955366670336?s=20) that the data available for download matched Michigan’s public records, and state officials confirmed that the voter data is publicly available to anyone through a Freedom of Information Act (FOIA) request. Similar claims circulated recently with voter data from Florida being posted on a Russian hacking forum. Again, [EIP verified](https://twitter.com/2020Partnership/status/1319034198250811392?s=20) that the data schema matched what is made public by the state.”

(EIP refers to the [Election Integrity Partnership](https://www.eipartnership.net/), a mix of academic, public and private sector institutions seeking to “detect and mitigate the impact of attempts to prevent or deter people from voting or to delegitimize election results.” The Stanford Internet Observatory is part of this consortium.)

**Election Administration Worries**

These efforts to create and spread false claims about voting and the underlying election system are in the sphere of media and partisan propaganda, which was not the same sphere as where elections are conducted. The world of running elections resembles an assembly line, where voters and ballots are methodically processed.

Since 2016, state and county election officials have taken [many steps](https://www.cisa.gov/protect2020) to monitor cyber attacks in real time and to harden their data and related computer systems, starting with voter registration files, said a former top state election official who spoke on background. In addition to using sensors to detect intrusions and quickly sharing activity reports with all states, access to voter data was limited, he said, even if some of that data was publicly available. Voter data was also backed up daily, he said, just as software was regularly updated with security patches.

Voter data was separated from vote-counting systems, he said. What was of more concern to him than claiming to meddle with registration data was the prospect of foreign agents infiltrating the private vendors who work for counties and states to “host and post” their election night results.

Disrupting the election night reporting is seen as a threat. Many election officials recall how the Democratic Party’s 2020 Iowa Caucus results were delayed for a day due to an app and system failure, creating much consternation including the mainstream media’s inability to explain the delay and urge the public to wait.

The New York Times recently [noted](https://www.nytimes.com/2020/10/23/us/elections/russia-poses-a-bigger-election-threat-than-iran-many-us-officials-say.html) that county election offices could be targets of [ransomware](https://www.nytimes.com/2020/09/27/technology/2020-election-security-threats.html), where systems are frozen until bounties were paid. That prospect was raised in an October 26 briefing by ex-Secretary of Homeland Security Michael Chertoff for the bipartisan [National Task Force on Election Crises](https://www.electiontaskforce.org/members). Microsoft had just obtained a court order to disable a ransomware network, Chertoff said.

There are other potential worries. In many primary states debuting new voting systems before the pandemic struck in March, electronic poll books—which help voters check in at precincts—[kept losing their online link](https://votingbooth.media/many-new-voting-systems-debuted-in-2020-arent-ready-for-prime-time/) to state voter databases. The spotty connectivity affected numerous California counties. Election officials in Georgia and South Carolina reported similar issues during October’s early voting. Should that issue recur or a ransomware threat emerge on November 3, the remedy would be distributing paper copies of voter rolls to precincts, experts have [said](https://www.nytimes.com/2020/09/27/technology/2020-election-security-threats.html).

Another point of vulnerability is the cellular modems that connect precinct ballot scanners to a central tabulator to report the election night’s vote totals. Ion Sancho, the former supervisor of elections (SOE) in Leon County, Florida, recently wrote a [letter](https://bradblog.com/Docs/IonSancho-LetterToSOEs-WirelessModems_102320.pdf) noting this concern to Florida’s SOEs and urging them to make other plans.

“[T]he ideal solution is to remove your central tabulator from the internet completely and to not use your wireless modems,” he [said](https://bradblog.com/Docs/IonSancho-LetterToSOEs-WirelessModems_102320.pdf), saying there were other ways to report precinct results. He suggested taking photos of the cash register-like poll tape produced at the close of voting and sending that image in via text or by email, or hand-delivering the vote-counting machinery’s computer memory card.

Any national election involving 10,000 jurisdictions, hundreds of thousands of poll workers and tens of thousands of pieces of machinery will have problems. Whether those problems accelerate to affect multitudes of voters or alter the vote counts is another matter—and at the heart of assessing threats to the election’s legitimacy.

What happens inside the election infrastructure is one thing, while what is said about those procedures in the media or in political propaganda is another.

“We are now in the final stretch of the election, and tens of millions of voters have already cast their votes free from foreign interference,” CISA’s Krebs said in a “[Rumor Control](https://www.cisa.gov/rumorcontrol)” video. “We remain confident that no foreign cyber actor can change your vote. And we still believe that it would be incredibly difficult for them to change the outcome of an election at the national level.”

“But that doesn’t mean various actors won’t try to introduce chaos in our elections and make sensational claims that overstate their capabilities,” he continued. “In fact, the days and weeks just before and after Election Day are the perfect time for our adversaries to launch efforts intended to undermine your confidence in the integrity of the electoral process.”

“The divisions within American society, and many others, are now so deeply ingrained that there’s no need for foreign influence in order to amplify and inflame,” [noted](https://www.lawfareblog.com/media-has-overcorrected-foreign-influence) Claire Wardle, a misinformation expert, on the national security blog [Lawfare](https://www.lawfareblog.com/). “From the cellphone-captured footage of Americans screaming in [supermarkets](https://www.youtube.com/watch?v=92ZRCl0uF1I) about masks, to [family members](https://www.buzzfeednews.com/article/janelytvynenko/qanon-families-friends) having to disown loved ones because of outlandish beliefs, to a [neutered Centers for Disease Control and Prevention](https://www.washingtonpost.com/health/2020/09/28/cdc-under-attack/) whose downfall was fueled by and consequently fueled misinformation, [to](https://www.theguardian.com/education/2020/mar/10/mccarthyism-uk-universities-academics-fear-shaming-for-leftwing-views) [university](https://theweek.com/articles/860278/worked-website-that-rated-professors-political-bias-what-learned) lecturers terrified of being filmed by students looking for evidence of liberal bias, to a weakened news media falling almost on a daily basis in the [trust ratings](https://www.journalism.org/2020/08/31/americans-see-skepticism-of-news-media-as-healthy-say-public-trust-in-the-institution-can-improve/), the evidence of our divided society is all around us.”

In other words, voters should expect competing and even false claims about the voting experience and the election results on November 3 and in the days after. While some of those claims will be amplified by foreign adversaries, most will originate domestically, where voters will have to wait for results, assess the evidence of accurate vote counts and live with the political consequences.