

Election Hackers Altered Voter Rolls, Stole Private Data, Officials Say

The hacking of state and local election databases in 2016 was more extensive than previously reported, including at least one successful attempt to alter voter information, and the theft of thousands of voter records that contain private information like partial Social Security numbers, current and former officials tell TIME.

In one case, investigators found there had been a manipulation of voter data in a county database but the alterations were discovered and rectified, two sources familiar with the matter tell TIME. Investigators have not identified whether the hackers in that case were Russian agents.

The fact that private data was stolen from states is separately providing investigators a previously unreported line of inquiry in the probes into Russian attempts to influence the election. In Illinois, more than 90% of the nearly 90,000 records stolen by Russian state actors contained drivers license numbers, and a quarter contained the last four digits of voters' Social Security numbers, according to Ken Menzel, the General Counsel of the [State Board of Elections](#).

Congressional investigators are probing whether any of this stolen private information made its way to the Trump campaign, two sources familiar with the investigations tell TIME.

"If any campaign, Trump or otherwise, used inappropriate data the questions are, How did they get it? From whom? And with what level of knowledge?" the former top Democratic staffer on the [House Intelligence Committee](#), Michael Bahar, tells TIME. "That is a crux of the investigation."

Spokesmen for the House and [Senate Intelligence](#) committees declined to comment on the search for stolen data. No one contacted for this story said they had seen evidence that the stolen, private, data had actually made its way to the Trump campaign.

The House Intelligence Committee plans to seek testimony this summer from Brad Parscale, the [digital director of the Trump campaign](#), CNN reported last week. Hill investigators in February asked the White House and law enforcement agencies to [ensure that all materials](#) relating to contacts between the Trump administration, transition team and campaign had with the Russians had been preserved. Parscale did not return messages requesting comment for this story. Trump's press secretary, [Sean Spicer](#), referred questions regarding the investigations to Trump's legal team, which did not respond to requests for comment.

Both intelligence committees are looking at whether and how the intrusions could have furthered Russia's larger strategic goals of undermining U.S. democracy, hurting Hillary Clinton and helping Donald Trump. During the run up to the vote, Obama Administration cyber-security officials took steps to prepare for [widespread voter registration manipulation](#), fearing Russia might seek to cause chaos at polling places to undermine the credibility of the election. Current and former law enforcement and intelligence officials say Russia could also have tried to use stolen voter data to gain leverage over witting or unwitting accomplices in the Trump camp, by involving them in a broader conspiracy.

The House and Senate Intelligence committees held hearings on June 22 to highlight the ongoing vulnerability of the U.S. election systems. "I'm deeply concerned," said North Carolina Republican Senator Richard Burr who chairs the Senate Intelligence Committee, that "we could be here in two or four years talking about a much worse crisis."

Cyber-security officials testifying at the Senate hearing acknowledged for the first time the extent of the Russian effort to interfere with the election. Twenty-one states saw such intrusions last year, a senior official from the Department of Homeland Security, Jeanette Manfra, said. None of the intrusions affected the vote count itself, all the officials testified.

That has not reassured some Hill leaders. “There’s no evidence they were able to affect the counting within the machines,” says the top Democrat on the House Intelligence committee, Congressman Adam Schiff of California. But, he added, “the effect on the election is quite a different matter.”

The Russian efforts against state and local databases were so widespread that top Obama administration cyber-security officials assumed that by Election Day Moscow’s agents had probed all 50 states. “At first it was one state, then three, then five, then a dozen,” says Anthony Ferrante, a former FBI cybersecurity official and member of the White House team charged with preparedness and response to the cyber intrusion. At that point, says Michael Daniel, who led the White House effort to secure the vote against the Russian intrusions, “We had to assume that they actually tried to at least rattle the doorknobs on all 50, and we just happened to find them in a few of them.”

Many hackers, including state-sponsored ones, use automated programs to target hundreds or even thousands of computers to check for vulnerabilities. But confirming intrusions is hard. As far as officials have been able to determine, the number of actual successful intrusions, where Russian agents gained sufficient access to attempt to alter, delete or download any information, was “less than a dozen,” current and former officials say. But that wasn’t the only worry.

“In addition to the threat to the vote we were also very concerned about the public confidence in the integrity of the electoral system,” says Ferrante.

Special Counsel Robert Mueller is investigating whether any laws were broken in relation to the Russian attack. The Congressional intelligence probes also seek to determine the nature and scope of the Russian espionage operation in order to protect future elections.

“The integrity of the entire system is in question,” says Bahar, “So you need the system to push back and find out what happened and why, so it never happens again.”