If Voting Machines Were Hacked, Would Anyone Know?

June 14, 20175:00 AM ET
Heard on Morning Edition

A ballot scanner in New York City ahead of last November's election.

Drew Angerer/Getty Images

As new reports emerge about Russian-backed attempts to hack state and local election systems, U.S. officials are increasingly worried about how vulnerable American elections really are.

While the officials say they see no evidence that any votes were tampered with, no one knows for sure.

Voters were assured repeatedly last year that foreign hackers couldn't manipulate votes because, with few exceptions, voting machines are not connected to the Internet. "So how do you hack something in cyberspace, when it's not in cyberspace?" Louisiana Secretary of State Tom Schedler said shortly before the 2016 election.

But even if most voting machines aren't connected to the Internet, says cybersecurity expert Jeremy Epstein, "they are connected to something that's connected to something that's connected to the Internet."

A recently leaked National Security Agency report on Russian hacking attempts has heightened concerns. According to the report, Russian intelligence services broke into an election software vendor's computer system and used the information it gained to send 122 election officials fake emails infected with malicious software. Bloomberg News reported Tuesday that Russia might have attempted to hack into election systems in up to 39 states.

While it's unclear if any of the recipients took the bait in the email attack, University of Michigan computer scientist Alex Halderman says it's just the kind of phishing campaign someone would launch if they wanted to manipulate votes.

"That's because before every election, the voting machines have to be programmed with the design of the ballots — what are the races, who are the candidates," says Halderman.

He notes that the programming is usually done on a computer in a central election office or by an outside vendor. The ballot program is then installed on individual voting machines with a removable memory card.

"So as a remote attacker, I can target an election management system, one of these ballot programming computers. If I can infect it with malicious software, I can have that malicious software spread to the individual machines on the memory cards, and then change votes on Election Day," says Halderman.

There's absolutely no evidence any of this happened in last year's election. But Halderman notes that some, or all, electronic voting machines in 14 states have no paper ballot backups that can be checked to make sure the electronic results are correct.

State and local election officials insist such an attack would be extremely difficult, if not impossible, because they've imposed tight security measures — including restrictions on who has access to voting equipment and repeated checks to make sure machines are working properly.

Still, Connecticut Election Director Peggy Reeves told a National Academies of Sciences, Engineering, and Medicine panel on Monday that many local election officials are ill-equipped to handle cybersecurity threats.

"Many of our towns actually have no local IT support," she said. "Seriously, they don't have an IT director in their town. They might have a consultant that they call on if they have an issue. So they look to us, but we're a pretty small division."

Reeves said the best protection against hackers is probably the fact that the nation's voting system is so decentralized, with different processes and equipment used in thousands of different locations.

Larry Norden, an election technology expert with the Brennan Center, agrees, but he's worried that hackers were laying the groundwork for more serious attacks when they probed voter registration databases, as Russia is accused of doing.

"This is a real threat," says Norden. "It's not going away, and if anything, foreign adversaries, even people at home, might be emboldened to do this more going forward. And to me it is a real call that we have to do more as soon as possible to secure these systems."

He and computer security experts, such as Halderman, think the best solution is to make sure all voting machines have paper records to back up the electronic results. They say states should also conduct audits after every election to make sure the electronic results match the paper ones. About half the states already do some audits, but Norden says most are inadequate.