Fortune Magazine:

What Is Election Hacking— And Can It Change Who Wins?

By Kartikay Mehrotra, Andrew Martin, And Bloomberg

December 26, 2019

Americans have relied on computers to tally votes since at least 1964, when two Georgia counties used them to count punch-card ballots in a primary election. Over time, high-tech election systems largely supplanted paper ballots and gear-and-lever machinary, a trend hastened by the contested 2000 presidential election between George W. Bush and Al Gore. (Remember hanging chads?) But ever-greater reliance on digital voter registration, electronic voting and computerized tabulation have created the opportunity, at least, for hackers to sabotage elections, and Americans aren't the only ones who are fearful.

1. What is meant by 'election hacking'?

It's sometimes used as a catch-all phrase to encompass all sorts of underhanded efforts to subvert elections, including the type of social media disinformation campaign undertaken by Russia to taint elections in the U.S., Europe and Africa. But in its most literal form, election hacking refers to computer breaches that are intended to manipulate voter data, change a vote tally or otherwise discredit tabulated results.

2. How could an election be hacked?

A hacker could reprogram an electronic voting machine directly, if it's left unguarded, or remotely, if it's connected to the internet. (A popular topic at hacker conferences is just how easy that would be to do.) Doing so undetected, and on a scale large enough to influence an election result, wouldn't be easy, as there are thousands of local jurisdictions with different voting methods and equipment. But hackers might only need to focus on a few key precincts in a swing state. Or they could alter a state's voter-registration data so that large numbers of voters get turned away at the polls. The wireless process of transmitting tabulated results to a local database is another possible target. Ransomware could be used in the days leading up to or on Election Day to hold the vote hostage. For anyone determined to do harm to the democratic process, a successfully hacked election could sow lasting mistrust in the voting process, whether or not it actually changes who wins.

3. Has hacking ever changed an election result?

It's hard to say for sure. One oft-cited example is the 2004 presidential race in Ukraine, in which Prime Minister Viktor Yanukovych won an election that was marred by allegations of fraud -- helping to trigger the Orange Revolution and a rerun of the vote. What can be said with more certainty is that election hacking has been attempted. A hacker allegedly tried to sabotage the first democratic election in South Africa in 1994, boosting vote tallies for far-right candidates; the breach was discovered and the vote tally delayed, with Nelson Mandela ultimately declared the winner. A brazen attempt to change the presidential vote in Ukraine in 2014 was attributed to a pro-Moscow hacking group that sabotaged Ukraine's central election computers days before the vote. Other election-related hacks occurred in Bulgaria in 2015 and in the Philippines in 2016.

4. How about in the U.S.?

There have been credible reports of malfunctions and mishaps with electronic voting machines; in local elections in Pennsylvania's Northampton County in November, touchscreen voting machines created such chaos that poll workers had to crack them open, remove the ballot records and use scanners summoned from across state lines to conduct a recount. (The maker of the machines, Election Systems & Software, the leading U.S. manufacturer of voting technology, apologized for what it called a "reporting issue" but assured voters that the results were accurate.) What's been lacking in U.S. cases is any evidence that errors and glitches were intentionally caused. U.S. officials say Russian hackers did probably make cyber-intrusions into election databases in all 50 states during the 2016 campaign, going so far as to extract data related to tens of thousands of voters in Illinois. But it's generally agreed that even then, Russian intelligence didn't disrupt voter rolls or change the vote.

5. Why didn't Russia manipulate results?

It's not clear, and the Russians certainly aren't saying. One possible explanation is that they didn't have time to master the U.S.'s complex voting system, which is spread over more than 7,000 local jurisdictions. Another is that a warning from the Obama administration -- which took the unprecedented step of complaining directly to Moscow over a modern-day "red phone" -- caused the Russians to back off. In its report on Russia interference in the election, the Senate Intelligence Committee offered still more theories: that the Russians may have sought to gather information for traditional espionage activities, or that they were cataloging options to use at a later date.

6. How big is the threat now?

In a joint statement looking ahead to the 2020 election, top U.S. security officials -- including Attorney General William Barr and National Security Agency Director Paul Nakasone -- warned that Russia, China, Iran and others "will seek to interfere in the voting process or influence voter perceptions." In testimony before Congress in July, Special Counsel Robert Mueller warned that Russia was still trying to undermine U.S. elections. "They're doing it as we sit here," he told lawmakers. That same month, Microsoft Corp. found that state-backed hackers had attempted to infiltrate targets related to U.S. elections more than 700 times in the previous year.

7. What other countries are contending with election hacking?

India and Brazil are among the large democracies that have joined the U.S. both in adopting electronic voting and worrying about how it might be manipulated. Estonia is among the leaders of electronic voting -- roughly a third of its citizens voted online in a recent election -- and its efforts are often cited as a model. But some other countries have run into problems with electronic voting. The Dutch adopted digital voting in the 1990s, then abolished it a decade later after activists showed how it was vulnerable to being hacked. More recently, Switzerland suspended a plan to expand electronic voting after security researchers found flaws in the system, including one that would have allowed an attacker to change votes.

8. What can be done?

Ohio says an attempted 2019 Election Day intrusion, which it traced to "a Russian-owned company," was thwarted because it triggered software that acts as a digital burglar alarm. Such sensors are now common in election systems in all 50 states. In addition, the vulnerabilities exposed in the 2016 U.S. election added fuel to a nationwide movement for localities to adopt voting machines that produce a paper trail, so results tabulated by computers can be checked by humans. There's an emerging standard for what's called a risk-limiting audit, which calls for a "statistically meaningful" number of ballots to be hand-counted. Cybersecurity experts are clamoring for jurisdictions to use hand-marked paper ballots instead of touchscreen voting machines called ballot-marking devices. Many election administrators are buying those machines anyway, contending that they're more efficient and easier to use than paper and pencil.