
A Single Person Could Swing an Election

(June 29, 2006) - Contributed by Zachary A. Goldfarb, Special to The Washington Post

Electronic Systems' Weaknesses May Be Counteracted With Audits, Report Suggests

This article was published by The Washington Post on June 28, 2006. To determine what it would take to hack a U.S. election, a team of cybersecurity experts turned to a fictional battleground state called Pennasota and a fictional gubernatorial race between Tom Jefferson and Johnny Adams. It's the year 2007, and the state uses electronic voting machines. Jefferson was forecast to win the race by about 80,000 votes, or 2.3 percent of the vote. Adams's conspirators thought, "How easily can we manipulate the election results?" The experts thought about all the ways to do it. And they concluded in a report issued yesterday that it would take only one person, with a sophisticated technical knowledge and timely access to the software that runs the voting machines, to change the outcome. The report, which was unveiled at a Capitol Hill news conference by New York University's Brennan Center for Justice and billed as the most authoritative to date, tackles some of the most contentious questions about the security of electronic voting.

The report concluded that the three major electronic voting systems in use have significant security and reliability vulnerabilities. But it added that most of these vulnerabilities can be overcome by auditing printed voting records to spot irregularities. And while 26 states require paper records of votes, fewer than half of those require regular audits. "With electronic voting systems, there are certain attacks that can reach enough voting machines . . . that you could affect the outcome of the statewide election," said Lawrence D. Norden, associate counsel of the Brennan Center.

With billions of dollars of support from the federal government, states have replaced outdated voting machines in recent years with optical scan ballot and touch-screen machines. Activists, including prominent computer scientists, have complained for years that these machines are not secure against tampering. But electronic voting machines are also much easier to use for disabled people and those who do not speak English.

Voting machine vendors have dismissed many of the concerns, saying they are theoretical and do not reflect the real-life experience of running elections, such as how machines are kept in a secure environment.

"It just isn't the piece of equipment," said David Bear, a spokesman for Diebold Election Systems, one of the country's largest vendors. "It's all the elements of an election environment that make for a secure election."

"This report is based on speculation rather than an examination of the record. To date, voting systems have not been successfully attacked in a live election," said Bob Cohen, a spokesman for the Election Technology Council, a voting machine vendors' trade group. "The purported vulnerabilities presented in this study, while interesting in theory, would be extremely difficult to exploit."

At yesterday's news conference, the push for more secure electronic voting machines, which has been popular largely on the left side of the political spectrum since the contested outcome of the 2000 presidential election in Florida, picked up some high-profile support from the other side.

Republican Reps. Tom Cole (Okla.) and Thomas M. Davis III (Va.), chairman of the House Government Reform Committee, joined Rep. Rush D. Holt (D-N.J.) in calling for a law that would set strict requirements for electronic voting machines. Howard Schmidt, former chief of security at Microsoft and President Bush's former cybersecurity adviser, also endorsed the Brennan report.