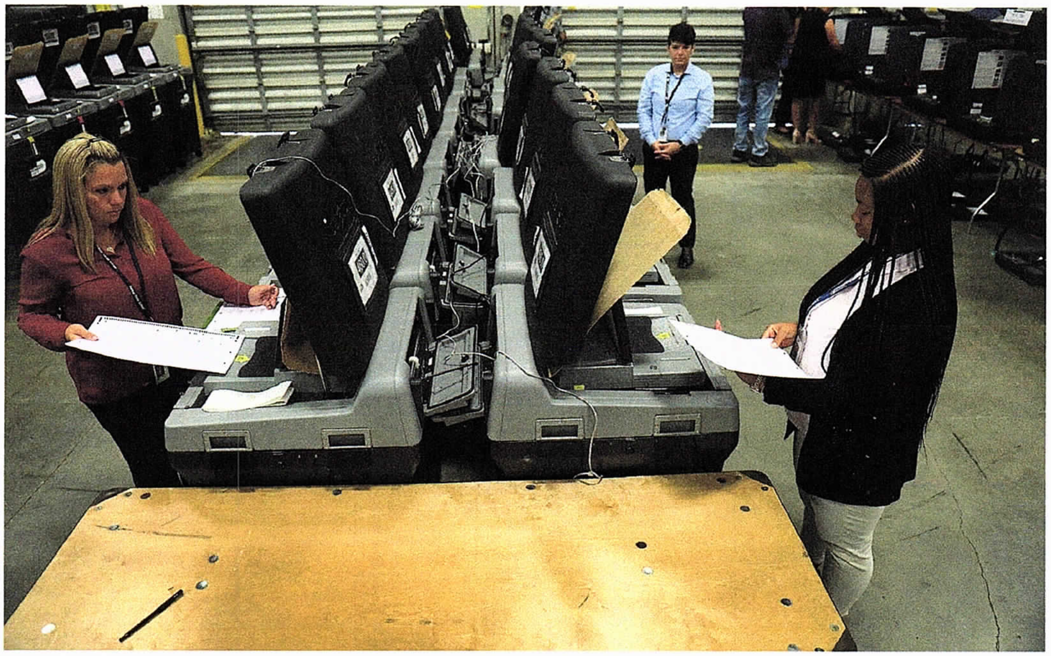
The New York Review of Books

Voting Machines: What Could Possibly Go Wrong?

Jennifer Cohn

November 5, 2018

The potential vulnerability of voting machines is critical because the entire system of our democracy depends on public trust—the belief that, however divided the country is, the result has integrity. Nothing is more insidious and corrosive than the idea that the tally of votes itself could be unreliable and exposed to fraud.



Joe Raedle/Getty Images

Miami-Dade election support specialists checking voting machines, Doral, Florida, August 8, 2018

Since the 2016 election, there has been a good deal of commentary and reporting about the threats to American democracy from, on the one hand, Russian interference by Facebook and Twitterbot-distributed propaganda, and on the other, voter ID laws and other partisan voter suppression measures such as electoral roll purges. Both of these concerns are real and urgent, but there is a third, yet more sinister threat to the integrity of the November 6 elections: the vulnerability of the voting machines themselves. This potential weakness is critical because the entire system of our democracy depends on public trust—the belief that, however divided the country is and fiercely contested elections are, the result has integrity. Nothing is more insidious and corrosive than the idea that the tally of votes itself could be unreliable and exposed to fraud.

Although election officials often claim our computerized election system is too "decentralized" to allow an outcome-altering cyber-attack, it is, in fact, centralized in one very important way: just two vendors, Elections Systems & Software, LLC, and Dominion Voting, account for about 80 percent of US election equipment. A third company, Hart Intercivic, whose e-slate machines have recently been reported to be flipping early votes in the current Senate race in Texas between Beto O'Rourke and Ted Cruz, accounts for another 11 percent. The enormous reach of these three vendors creates an obvious vulnerability and potential target for a corrupt insider or outside hacker intent on wreaking havoc.

These vendors supply three main types of equipment that voters use at the polls: optical or digital scanners for counting hand-marked paper ballots, direct record electronic (usually touchscreen) voting machines, and ballot-marking devices that generate computer-marked paper ballots or "summary cards" to be counted on scanners.

Contrary to popular belief, all such equipment can be hacked via the Internet because all such equipment must receive programming before each election from memory cards or USB sticks prepared on the county's election management system, which connects to the Internet. Thus, if an election management system is infected with malware, the malware can spread from that system to the memory cards and USB sticks, which then would transfer it to all voting machines, scanners, and ballot-marking devices in the county.

Malicious actors could also attack election management systems via the remote access software that some vendors have installed in these systems. ES&S, which happens to have donated more than $30,000 to the Republican State Leadership Council since 2013, admitted earlier this year that it has installed remote access software in election management systems in 300 jurisdictions, which it refuses to identify. And in August 2004, as reported by bradblog.com, the United States Computer Emergency Readiness Team released a Cyber Security Bulletin concerning the Diebold GEMS central tabulator, stating that "a vulnerability exists due to an undocumented backdoor account, which could [allow] a local or *remote* authenticated user [to] modify votes [emphasis added]." This central tabulator was used to count one-third of the votes in 37 states in the 2004 election.

The memory cards or USB sticks used to transfer the pre-election programming from the election management system to the voting machines, scanners, and ballot-marking devices constitute another potential attack vector. In theory, the person who distributes those cards or USB sticks to the precincts could swap them out for cards containing a vote-flipping program.

Memory cards are also used in the reverse direction—to transfer precinct tallies from the voting machines and scanners to the election management system's central tabulator, which aggregates those tallies. Problems can occur during this process, too. During the 2000 presidential election between George W. Bush and Al Gore, for example, a Global/Diebold machine in Volusia County, Florida, subtracted 16,000 Gore votes, while adding votes to a third-party candidate. The "Volusia error," which caused CBS news to call the race prematurely for Bush, was attributed to a faulty memory card, although election logs referenced a second "phantom" card as well. As noted recently in the *New York Times Magazine*, questions from this disturbing episode remain unanswered, such as "[W]hat kind of faulty card deleted votes only for Gore, while adding votes to other candidates?" The incident, however, slipped from public consciousness amid the hoopla over hanging chads and butterfly ballots.

Further complicating matters, some jurisdictions transfer results from the precincts to the central tabulators via cellular modems. ES&S has recently installed such cellular modems in Wisconsin, Florida, and Rhode Island. Michigan and Illinois transfer results via cellular modem as well. According to Computer Science Professor Andrew

Appel of Princeton University, these cellular modems could enable a malicious actor to intercept and "alter vote totals as they are uploaded" by setting up a nearby cell phone tower (similar to the Stingray system used by many police departments).

After precinct tallies are sent by memory card or modem to the central tabulators, a memory card or flash drive transfers the aggregated totals from the central tabulators to online reporting systems, creating another hacking opportunity. In Georgia, a flash drive transfers results from the central tabulator to the online election night reporting system, and the same flash drive is then reinserted into the tabulator for the next round of memory cards. As explained by election integrity advocate Marilyn Marks, that is like "sharing needles."

Central scanners, which are used to count absentee ballots and paper ballots from polling places that lack precinct-based scanners, are also vulnerable. As a video produced by the Emmy award-winning journalist and filmmaker Lulu Friesdat has demonstrated, the ES&S 650 central scanner, which is used in twenty-four states, can be rigged to flip votes within one minute of direct access.

As troubling, voting machines themselves can be compromised within seven minutes of direct access, with little more than a screwdriver and a new ROM chip. According to computer science Professor Richard DeMillo of the Georgia Institute of Technology, voting machines are often left unattended for long periods: "We have pictures of [my colleagues] walking into gymnasiums with access to the [voting machines] that are left unattended overnight." And as DeMillo explained, if a single voting machine is infected, the virus can spread to the election management system's central tabulator, which aggregates all precinct tallies in the county, via the magnetic cards that are plugged into every machine to accumulate the results.

Vote flipping aside, malicious or benign actors can also cause electronic failure that prevents the machines from working at all. The potential impact of electronic failure is far greater with touchscreen systems, whether for voting machines or ballot-marking devices, than with hand-marked paper ballots counted on scanners because, when touchscreens fail, voters may have no means of voting whatsoever. In 2008, for example, voters in Horry County, South Carolina, were forced to vote on scraps of paper when touchscreen voting machines malfunctioned in 80 percent of the county's precincts. A State Election Commission spokesperson was quoted telling people to vote on paper towels if necessary. In 2016, improperly coded memory cards caused most of the machines in Washington County, Utah, to break down. Poll sites offered backup paper ballots, until some ran out and told voters to return later.

Touchscreen machines are also known to cause long lines because they limit the number of voters who can vote at any one time to the number of touchscreens available at the polling place. Again, this contrasts with hand-marked paper ballots and scanners, where the only limit to the number of people who can fill in their ballots concurrently is the number of pens and paper ballots at the polling station.

Electronic poll books, the tablets and laptops that many jurisdictions now use to check voter registrations at the polls, are also of grave concern. The journalist and radio show host Brad Friedman, who has investigated and written about our computerized election system for almost two decades, warns that if electronic poll books "go down, and these places don't have paper backups, it will be a disaster... [In the case of] a denial of service attack meant to knock out the Internet on election day, what do you do? There are no do-overs in elections."

We know what this might look like because on election day 2016 in Durham County, North Carolina, problems with the county's poll books resulted in hundreds of calls from irate voters, many of whom were turned away at the polls, even when they displayed current registration cards. VR Systems, the Florida-based company that manufactured the poll books in Durham County, and which also supplies poll books to California, Florida, Indiana, North Carolina, New York, and Virginia, was hacked in August 2016 in a Russian spear-phishing attack. In 2017, current and former intelligence officials said that hackers had also breached at least two other providers of critical election services before the 2016 election, but would not disclose the names of the two other providers.

USA Today reported in August last year that ES&S, which by itself accounts for about 44 percent of US election equipment, had left database files online and publicly available on an Amazon AWS cloud server for an "undetermined amount of time," including "encrypted versions of passwords for ES&S employee accounts." The database was discovered by a cybersecurity company called Upguard, which advised that "the encryption was strong enough to keep out a casual hacker but by no means impenetrable." According to *USA Today*, "configuring the security settings for Amazon's AWS cloud service is up to the user," and the "default for all of AWS' cloud storage is to be secure, so someone within ES&S would have had to choose to configure it as public."

The most worrisome aspect of all these various vulnerabilities is that—should they be exploited—we will be unable to prove whether and to what extent they have affected the outcome of an election. The effect of even very visible problems, such as long lines, voter registration issues, and electronic failures, is difficult to quantify. Moreover, machine vendors claim proprietary ownership of their software and hardware, precluding forensic analysis. After the 2016 election, the Department of Homeland Security confirmed that it had conducted no such analysis.

Thus the only way to know if foreign or domestic actors have altered electronic tallies is to conduct what statistics Professor Philip Stark of the University of California at Berkeley calls "evidence-based elections." This would involve a robust manual audit or manual recount of the paper ballots (or other paper record that the voter has reviewed for accuracy), and a secure chain of custody between the election night count and any audit or recount.

United States elections are not evidence-based elections. According to computer science Professor Alex Halderman of the University of Michigan, only two states, Colorado and New Mexico, conduct manual audits sufficiently robust to detect vote tally manipulation. More than half of US states do not require manual audits at all, while manual recount laws typically allow automatic state-funded recounts only if the margin of victory is less than 1 percent.

Depending on the type of voting system used at the polls, some jurisdictions may have no paper ballots (or other paper records) with which to conduct a manual recount or manual audit or recount in the first place. As of April 2018, fourteen states still used such "paperless" voting machines.

In the past few years, some jurisdictions have finally dumped their aging voting machines. But an alarming number—including counties in Kentucky, West Virginia, Arkansas, Tennessee, Delaware, Kansas, Michigan, Wisconsin, and Texas—have replaced the machines not with hand-marked paper ballots and scanners, but rather with ballot-marking devices and scanners. Although ballot-marking devices have long been used to serve the disabled community, the new versions are intended for so-called universal use. Like traditional touchscreen voting machines, they put a hackable touchscreen computer between the voter and his or her ballot.

These universal use ballot markers generate a summary card that some officials call a "paper ballot." The idea is that the voter can review the text on the summary card to confirm that it is accurate, so that the card can provide the basis for a manual audit or recount. But a recent study (awaiting peer review) by computer science Professor Richard DeMillo of the Georgia Institute of Technology and Marilyn Marks of the Coalition for Good Governance suggests that "in actual polling place settings, most voters do not try to verify paper ballot summaries, even when directed to do so," and that "among those voters who attempt to review their ballots, a statistically significant fraction... fail to recognize errors."

Thus, even if we had effective manual audit laws, our use of voting machines and universal-use ballot-marking devices would preclude reliable manual audits. As Friedman laments, "We do not have a system where supporters of the winners and the losers can walk away and *know* that the election was legitimately won or lost."

There are still steps, however, that voters and candidates can and should take before and during the midterm elections to protect their votes and voter registrations, many of which I have compiled into a handout. And as the Brennan Center for Justice advises, voters should also seek confirmation from their local election officials that the requisite emergency measures are in place should technical problems arise on election day.

Beyond the midterms, voters must pressure Congress to pass substantive election security legislation. A good example already before Congress is Senator Ron Wyden's Protecting American Votes and Elections Act, which would require all states to give voters the option to mark their ballots by hand and to carry out robust audits. The hand-marked ballot option is important because it prevents states from forcing voters to use voting machines or ballot-marking devices. Voters must also pressure their state lawmakers to implement similar election security laws to protect elections.

False assurances about election security will not suffice. If lawmakers expect voters to believe in the integrity of America's election system, then they must *make* the system secure and dispense with the complacent notion that the only threat is from a foreign adversary. As Friedman says, "[Y]ou do not need to be a fancy state-sponsored hacking organization to do it. It's one guy on the inside, whether an election official, or a voting machine company, or contractor, or whatever... It doesn't take a nation state to flip an election."

An earlier version of this essay misstated which year ES&S's donations to the Republican State Leadership Council started; it was 2013, not 2014.

Jennifer Cohn

Jennifer Cohn, an attorney, is an election integrity advocate and writer. (November 2018)