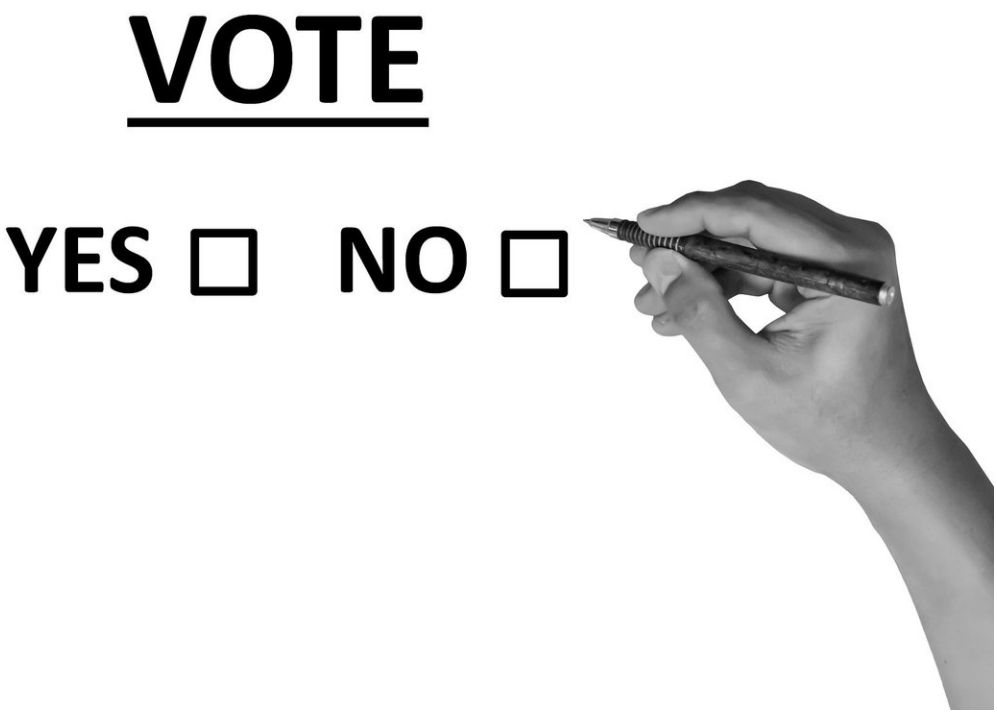
Four ways to defend democracy and protect every voter's ballot

September 6 2018, by Douglas W. Jones



Credit: CC0 Public Domain

As voters prepare to cast their ballots in the November midterm

elections, it's clear that U.S. voting is under electronic attack. Russian government hackers probed some states' computer systems in the runup to the 2016 presidential election and are likely to do so again – as might hackers from other countries or nongovernmental groups interested in sowing discord in American politics.

Fortunately, there are ways to defend elections. Some of them will be new in some places, but these defenses are not particularly difficult nor expensive, especially when judged against the value of public confidence in democracy. I served on the Iowa board that examines voting machines from 1995 to 2004 and on the Technical Guidelines Development Committee of the United States Election Assistance Commission from 2009 to 2012, and Barbara Simons and I coauthored the 2012 book "Broken Ballots."

Election officials have an important role to play in protecting election integrity. Citizens, too, need to ensure their local voting processes are safe. There are two parts to any voting system: the computerized systems tracking voters' registrations and the actual process of voting – from preparing ballots through results tallying and reporting.

Attacking registrations

Before the passage of the Help America Vote Act of 2002, voter registration in the U.S. was largely decentralized across 5,000 local jurisdictions, mostly county election offices. HAVA changed that, requiring states to have centralized online voter registration databases accessible to all election officials.

In 2016, Russian government agents allegedly tried to access voter registration systems in 21 states. Illinois officials have identified their state as the only one whose databases were, in fact, breached – with information on 500,000 voters viewed and potentially copied by the

hackers.

It's not clear that any information was corrupted, changed or deleted. But that would certainly be one way to interfere with an election: either changing voters' addresses to assign them to other precincts or simply deleting people's registrations.

Another way this information could be misused would be to fraudulently request absentee ballots for real voters. Something like that happened on May 29, 2013, when Juan Pablo Baggini, an overzealous campaign worker in Miami, used his computer to file online absentee ballot requests on behalf of 20 local voters. He apparently thought he had their permission, but county officials noticed the large number of requests coming from the same computer in a short period of time. Baggini and another campaign worker were charged with misdemeanors and sentenced to probation.

A more sophisticated attack could use voters' registration information to select targets based on how likely they are to vote a particular way and use common hacking tools to file electronic absentee ballot requests for them – appearing to come from a variety of computers over the course of several weeks. On Election Day, when those voters went to the polls, they'd be told they already had an absentee ballot and would be prevented from voting normally.

Two defenses for voter registration

There are two important defenses against these and other types of attacks on voter registration systems: provisional ballots and same-day registration.

When there are questions about whether a voter is entitled to vote at a particular polling place, federal law requires the person be issued a

provisional ballot. The rules vary by state, and some places require provisional voters to bring proof of identity to the county election office before their ballots will be counted – which many voters may not have time to do. But the goal is that no voter should be turned away from the polls without at least a chance their vote will count. If questions arise about the validity of the registration database, provisional ballots offer a way to ensure every voter's intent is recorded for counting when things get sorted out.

Same-day voter registration offers an even stronger defense. Fifteen states allow people to register to vote right at the polling place and then cast a normal ballot. Research on same-day registration has focused on turnout, but it also allows recovery from an attack on voter registration records.

Both approaches do require extra paperwork. If large numbers of voters are affected, that could cause long lines at polling places, which disenfranchise voters who cannot afford to wait. And like provisional voting, same-day registration may have more stringent identification requirements than for people whose voter registrations are already on the books. Some voters may have to go home to get additional documents and hope to make it back before the polls close.

Further, long lines, frustrated voters and frazzled election workers can create the appearance of chaos – which can play into the narratives of those who want to discredit the system even when things are actually working reasonably well.

Paper ballots are vital

Election integrity experts agree that voting machines can be hacked, even if the devices themselves are not connected to the internet.

Voting machine manufacturers say their devices have top-notch protections, but the only truly safe assumption is that they have not yet found additional vulnerabilities. Properly defending voting integrity requires assuming a worst-case scenario, in which every computer involved – at election offices, vote-tallying software developers and machine makers – has been compromised.

The first line of defense is that in most of the U.S., people vote on paper. Hackers can't alter a hand-marked paper ballot – though they could change how a computerized vote scanner counts it, or what preliminary results are reported on official websites. In the event of a controversy, paper ballots can be recounted, by hand if needed.

Conduct post-election audits

Without paper ballots, there is not a way to be completely sure voting system software hasn't been hacked. With them, though, the process is clear.

In a growing number of states, paper ballots are subject to routine statistical audits. In California, post-election audits have been required since 1965. Iowa allows election officials who suspect irregularities to initiate recounts even if the result appears decisive and no candidate asks for one; these are called administrative recounts.

Based on that experience, some election officials have told me that they suspect the current generation of scanners may be misinterpreting 1 vote in 100. That might seem like a small problem, but it's really way too much opportunity for error. Voting simulations show that changing just one vote per voting machine across the United States could be enough to allow an attacker to determine which party controls Congress.

Recounts are expensive and time-consuming, though, and can create illusions of disarray and chaos that reduce public confidence in the election's outcome. A better method is called a risk-limiting audit. It's a straightforward method of determining how many ballots should be randomly selected for auditing, based on the size of the election, the margin of the initial result and – crucially – the statistical confidence the public wants in the final outcome. There are even free online tools available to make the calculations needed.

Preliminary experiences with risk-limiting audits are quite promising, but they could be made even more attractive by small changes to ballot-sheet scanners. The main problem is that the method is based in math and statistics, which many people don't understand or trust. However, I believe relying on verifiable principles that any person could learn is far better than believing the assurances of companies that make voting equipment and software, or election officials who don't understand how their machines actually work.

Elections must be as transparent and simple as possible. To paraphrase Dan Wallach at Rice University, the job of an election is to convince the losers that they lost fair and square. The declared winners will not ask questions and may seek to obstruct those who do ask. The losers will ask the hard questions, and election systems must be transparent enough that the partisan supporters of the losers can be convinced that they indeed lost. This sets a high standard, but it is a standard that every democracy must strive to meet.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation