The New York Times | https://nyti.ms/2hpTy7w

The Opinion Pages | OP-ED CONTRIBUTORS

To Protect Voting, Use Open-Source Software

By R. JAMES WOOLSEY and BRIAN J. FOX AUG. 3, 2017

Although Russian hackers are reported to have tried to disrupt the November election with attacks on the voting systems of 39 states, the consensus of the intelligence community is that they were probably unsuccessful in their efforts to delete and alter voter data. But another national election is just 15 months away, and the risk that those working on behalf of President Vladimir Putin of Russia could do real damage — and even manage to mark your ballot for you or altering your vote — remains.

Since the debacle of the 2000 election (remember hanging chads?) American election machinery has been improved to reduce the chances of mis-tallying votes, outright fraud and attacks by hackers. These improvements brought with them a new concern: lack of software security. Most voting machines' software can now be easily hacked. This is in large part because the current voting systems use proprietary software based on Microsoft's operating system.

One post-2000 change — a useful one — was to move away from all-electronic touch-screen balloting, with no paper record indicating how someone voted. Nearly half of voters are registered in jurisdictions that use optical-scan systems that read marked paper ballots and tally the results. But one-quarter of voters still use direct-recording electronic voting machines, which produce no paper trail.

At polling places where voting machines don't provide this backup record, there's no way for election officials to run an effective recount if the electronics are

hacked.

That's why the National Association of Voting Officials is leading a movement to encourage election officials to stop the purchase of insecure systems and begin to use software based on open-source systems that can guard our votes against manipulation.

But there's resistance to this obvious solution. Microsoft and companies that bob along in its wake don't want their proprietary voting systems replaced by open-source software balloting systems, have aggressively lobbied against them.

Open-source software is simply software for which the original source code is made freely available and may be redistributed and modified. In the case of voting, open-source software systems would be overseen by public-private partnerships between counties and vendors.

Open-source systems are tried and tested. A majority of supercomputers use them. The Defense Department, NASA and the United States Air Force all use open-source systems, because they know this provides far more security. Every step in our voting process should use software that follows these examples.

Despite its name, open-source software is less vulnerable to hacking than the secret, black box systems like those being used in polling places now. That's because anyone can see how open-source systems operate. Bugs can be spotted and remedied, deterring those who would attempt attacks. This makes them much more secure than closed-source models like Microsoft's, which only Microsoft employees can get into to fix.

One reason for the software companies' resistance is the belief that it's impossible to make a profit from open-source software. This is a myth. Businesses that use open-source software still need all of the other things that software companies provide. Many major companies use open-source software in their products.

Open-source systems are already playing a role in some elections. New Hampshire has used them to allow disabled voters to fill out ballots online or on

their phones, while Travis County in Texas, San Francisco and Los Angeles have allocated funds to move toward open-source voting systems.

If the community of proprietary vendors, including Microsoft, would support the use of open-source model for elections, we could expedite progress toward secure voting systems.

With an election on the horizon, it's urgent that we ensure that those who seek to make our voting systems more secure have easy access to them, and that Mr. Putin does not.

R. James Woolsey is a former director of the Central Intelligence Agency. Brian J. Fox, the creator of the Bash open-source software, is the lead technologist of the National Association of Voting Officials and the California Association of Voting Officials, which develop open-source voting systems for use in public elections.

Follow The New York Times Opinion section on Facebook and Twitter (@NYTopinion), and sign up for the Opinion Today newsletter.

A version of this op-ed appears in print on August 3, 2017, on Page A19 of the New York edition with the headline: To Protect Voting, Use Open-Source.
