To the Editor April 20, 2020

Secure our Voting Machines

Are our voting results accurate? That is a very good question.

There has been a lot of attention paid to what many believe is nonexistent voter fraud, but precious little to cybersecurity in voting machines, and vote hacking following problems in the 2016 election. In fact, in some ways we appear to be going backwards on this issue.

Reality Winner was convicted of leaking classified info to the media about 2016 election hacking by the Russians, which was unknown to the public at the time. In 2018, Winner was sentenced to five years and three months in prison for violating the Espionage Act. Prosecutors said her sentence was the longest ever imposed in federal court for an unauthorized release of government information to the media. (More on this in a letter yet to come.)

After Russian hackers made extensive efforts to infiltrate the American voting apparatus in 2016, some states moved to restrict internet access to their vote-counting systems. Colorado got rid of barcodes used to electronically read ballots. California tightened its rules for electronic voting machines that can go online. Ohio bought new voting machines that deliberately excluded wireless capabilities.

America Won't Give Up Its Hackable Wireless Voting Machines

Michigan went in a different direction, authorizing as much as $82 million for machines that rely on wireless modems to connect to the Internet. State officials justified the move by saying it is the best way to satisfy an impatient public that craves instantaneous results, even if they're unofficial. https://www.bloomberg.com/news/articles/2020-01-03/america-won-t-give-up-its-hackable-wireless-voting-machines

Wisconsin Among Most Vulnerable Election Hacking States: Report

A new report authored by Congressional Democrats says that Wisconsin is one of 18 states with serious election-hacking vulnerabilities. https://patch.com/wisconsin/across-wi/wisconsin-among-most-vulnerable-election-hacking-states-report

Voters Fail Mock Election, Exposing Vulnerability to Hackers

There's a secret weapon in America's battle to secure the 2020 vote from nation-state hackers: the voters. But there's a problem. Only a few of them are in on the secret.

Many voters across the country will cast ballots this year on machines called ballot-marking devices, which use touchscreen technology with a paper trail. To ensure the accurate translation of each voter's choices from screen to paper, voters must verify ballot receipts to identify errors. There are two problems with this:

1. Ballot-marking machines rely on voters to check their work
2. Study finds that voters are too trusting of technology, and don't check their ballots

https://www.bloomberg.com/news/articles/2020-01-08/voters-fail-mock-election-exposing-vulnerability-to-hackers

We should all be concerned about this.