# Cyber Experts Warn of Major Election Vulnerabilities Going into 2020

*Randy DeSoto*
Published April 29, 2020 at 6:08am

With the November elections quickly approaching, election security experts are warning that the United States is very vulnerable to cyberattacks that could change the results of races, including the presidential contest.

Further, some simple changes could be made that would do much to ensure accurate election reporting, the experts say.

Harri Hursti — one the the world's foremost election security experts — observed in his newly released HBO documentary, "Kill Chain: the Cyber War on America's Elections," that due to the way electronic voting is conducted and the results reported throughout the United States, the system is vulnerable to hacking.

"The problem is once you understand how everything works, you understand how fragile everything is," Hursti says in the film.

"I keep hearing that the system is unhackable. Everything is hackable, always," the cyber expert added.

**TRENDING:** NBC Admits to Airing Highly Deceptive Edit of Attorney General Barr's Comments

Hursti famously demonstrated to Florida election officials just how easy it was to overwrite voting machine software to change results for his 2006 documentary film, "Hacking Democracy."

Last month, he told WCBS: "The most frightening thing is that from 2006 to now, nothing changed. The actual software that I hacked in 2005 is still in use. Those machines are still in 20 states."

Beyond the vulnerability of voting machines themselves to hacking, other vulnerabilities exist in the tallying and transmission of the results.

Do you support paper ballots and risk-limiting audits of election results?

Two of the biggest misconceptions Americans likely have about how elections are conducted are that votes are counted by state and local election officials and that the vote tallies themselves, even if backed up by paper ballots, are not vulnerable to hacks.

In October 2016, then-President Barack Obama made the oft-repeated argument that due to the decentralized nature of voting in the United States, elections, especially at the presidential level, cannot be hacked or significantly altered.

"There is no serious person out there who would suggest somehow that you could even rig America's elections in part because they are so decentralized and the numbers of votes involved," Obama said.

Election security expert Russell Ramsland told The Western Journal Americans need to understand that state and local officials, by and large, do not count the votes on election night, but have contracted private companies to do so.

"It is incredible how many people believe that their county or their state run their elections," Ramsland said. "They have no idea that all elections are actually conducted by private companies, with virtually no oversight, no transparency."

**RELATED:** Amy Klobuchar Issues Threat Against Republicans if Vote-by-Mail Is Not Funded

"And that private company writes the software, makes and sells the machines, keeps all the voter rolls, and tallies all the votes and reports them," he added. "It's totally and completely jobbed out to a private company with private shareholders."

Far from being decentralized, there are three main companies that tally the votes for election officials, according to "Kill Chain": Election Systems & Software, Dominion Voting Systems and Hart Voting Systems.

Hursti noted that none of these companies agreed to be interviewed for "Kill Chain."

There are "commonalities" between all the major companies in their election night reporting, he told The

Western Journal.

One thing all the electronic voting systems have in common is a removable drive or memory device, which engages in two-way communication with the database when results from each voting machine are uploaded.

Hursti explained that all these devices are programmed how to organize and communicate the data to the central database.

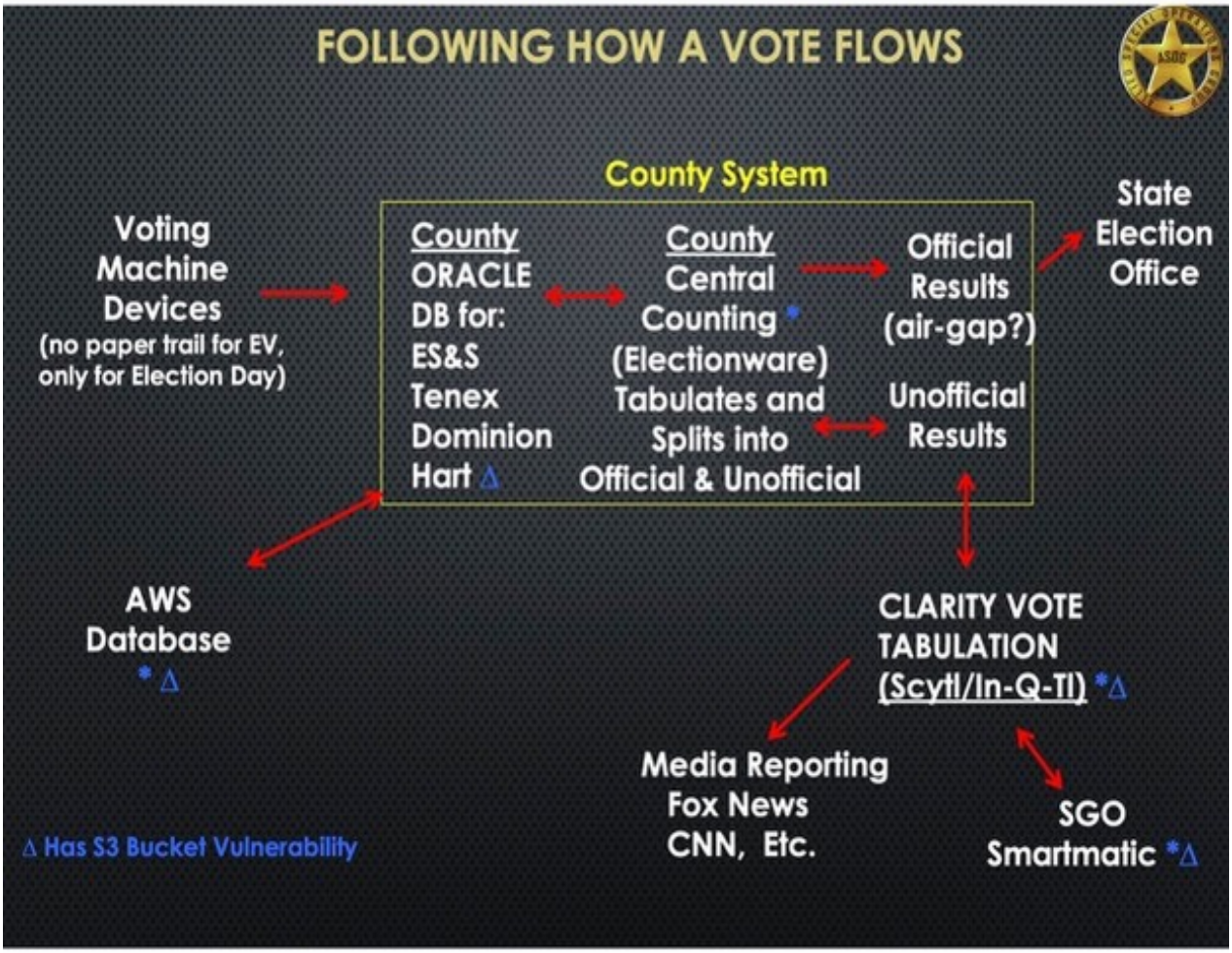
"The memory cards actually have a programming side," he said. "Programming can have a lot of logic. So the program can dynamically look [at] what is happening and decide on the spot what is needed to be done in this precinct on this machine" as part of changing the overall result.

"Once you can send that instruction to the election management system, the election management system is sending the same programming into every voting machine," Hursti continued.

"So the only thing you need to do is to modify that program, and there are so many different ways."

Ramsland created a diagram (shown below) to illustrate how votes typically flow from the precinct voting machines to databases maintained by companies like ES&S, Dominion and Hart to be tallied for the election results.

All this information travels over the internet to different databases (as signified by the blue triangles) along the way, which can be hacked.




The "unofficial results" are then made public through companies like Clarity Elections, which is the U.S. division of the Barcelona, Spain-based company Scytl.

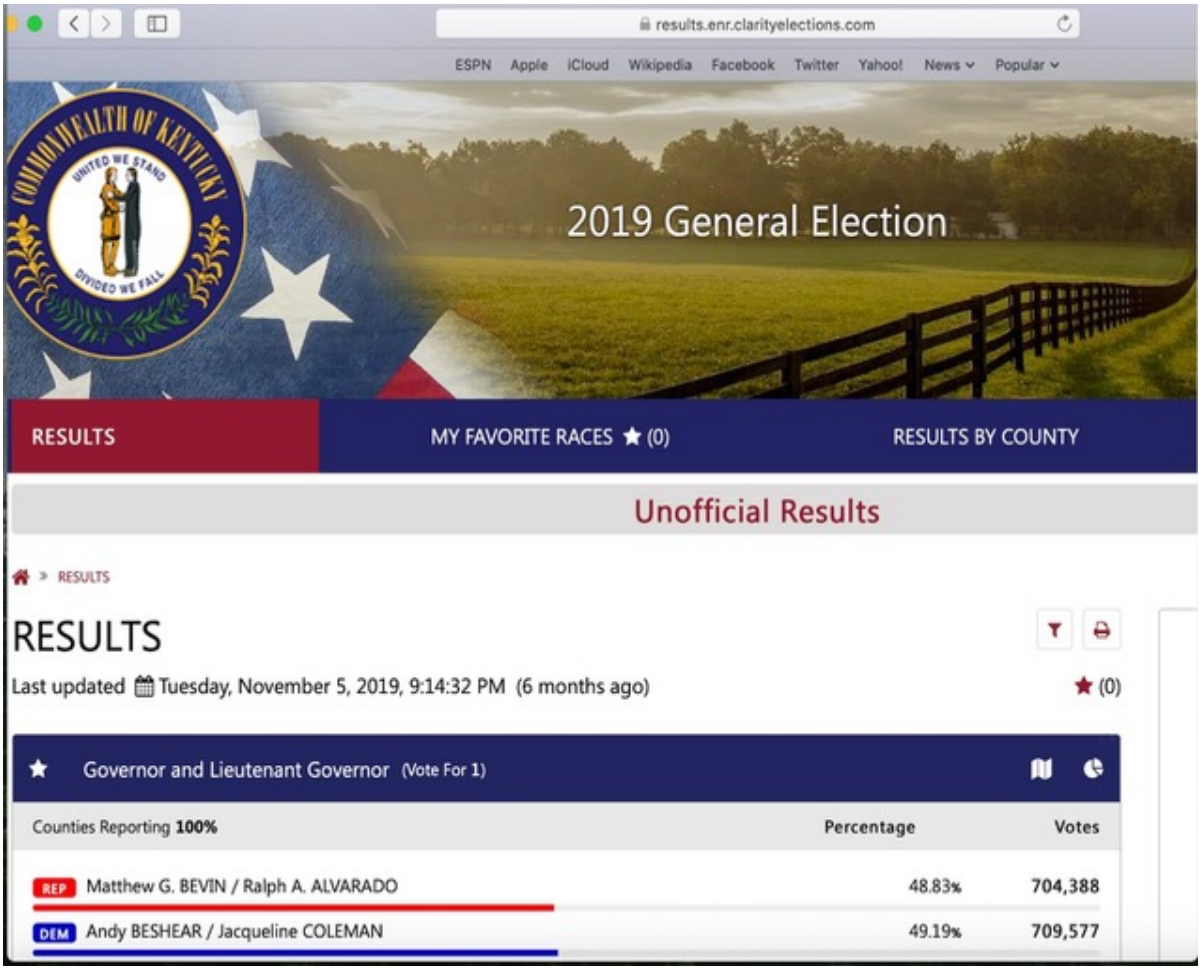
The company proudly states on its website that it has "successfully delivered election modernization projects in the US since 2008, and most recently for the 2018 Midterm Elections, when over 70 [million] voters from more than 900 U.S. counties successfully leveraged Scytl's technology."

The “unofficial results” are then made public through companies like Clarity Elections, which is the U.S. division of the Barcelona, Spain-based company Scytl.

The company proudly states on its website that it has “successfully delivered election modernization projects in the US since 2008, and most recently for the 2018 Midterm Elections, when over 70 [million] voters from more than 900 U.S. counties successfully leveraged Scytl’s technology.”

Kentucky is one of its customers, which can be seen in the election results from last fall’s gubernatorial race between Democrat Andy Beshear and then-Republican incumbent Matt Bevin.

Beshear edged out Bevin by less than a percentage point.



According to Hursti, one of the problems with the relatively new trend of private companies running elections is the inability of election officials to provide adequate oversight.

"The election services company tells how the show is run," he said, pointing out that those overseeing the election are often elected officials themselves, who may have very little or no IT expertise.

Nonetheless, he said, "the elected official, who does not know what is going on, is legally responsible" for the overall election results.

There would seem to be a perverse incentive if a hack were discovered by the private company not to report it or the extent of it to election officials, so as to not hurt the company's reputation and its potential opportunity to run future contests.

At the same time, the motivation is high for hostile actors (whether they be foreign powers, or political or business interests) to try to rig the outcome for their favored candidates or to simply sow seeds of distrust in the election process.

For his documentary "Kill Chain," Hursti traveled to Juneau, Alaska, to investigate the hacking of the state's Division of Election's website on election night in November 2016.

The Associated Press reported that election officials determined the India-based hacker did not manipulate any information.

Hursti believes — based on a review of documents obtained by a Freedom of Information Act request — the truth in terms of the extent of the breach was "likely ... clearly worse" than what the officials admitted.

"There was no containment in effect," he said in the documentary.

He then went to India to speak with the hacker, known as CyberZeist, who took credit for the breach.

"I had root access, which just not only allowed me access to make small changes, but granted me full access of the system," including the real-time data to the presidential race, the hacker said.

"I could have made any changes in the system," he added. "I could alter any data, any vote."

CyberZeist chose not to out of fear of being caught, recounting that he reasoned, "Do not edit anything. Just see what is going on. Then we can plan or take out or execute our next steps."

Hursti thinks the hacker likely deployed a cyber tool in the Alaska Division of Elections website.

CyberZeist told the documentarian that Russian interests are seeking to scan state election servers throughout the United States.

The AP reported in September 2017 that the Department of Homeland Security notified 21 states that attempts had been made to hack their election systems during 2016 election cycle.

Among those hit were the key battleground states of Florida, Ohio, Pennsylvania, Virginia and Wisconsin.

Ramsland explained that cyberattackers, whether they are working for the Russian government or some other entity, would likely just need to focus their efforts on a few key states like these to change the outcome of the 2020 presidential race.

"So if you want to change the presidency of this country, all you really have to do is put your whole team on making sure that your guy wins precinct by precinct in at least a semi-believable number in five states and probably only the big metropolitan areas of five states," he said.

Republican Sen. James Lankford of Oklahoma is among the bipartisan supporters of some key election reforms, most importantly the ability to verify the results of a contest.

Last summer, Lankford spoke out in opposition to Democratic Sen. Amy Klobuchar's "Election Security Act" on the grounds that it contained a partisan provision, but agreed with her on the importance of paper ballots and other cyber protection measures.

"Every state, every precinct, should be able to verify [an election], to be able to go to back to the people in their area and to say, 'This is how you voted, and this is how we verified the number is accurate.'"

"It's not just about the voting machine, or it's not just about the piece of paper," he added. "It's how it's counted, how it's presented, how the unofficial results even go out from the state the night of the election. All those things matter."

“Every state should have a system with a backup paper ballot,” Lankford said. “Every state, every precinct. Right now, that’s not so.”

Hursti and Ramsland agreed that human readable paper ballots must be required.

Some states and precincts use voting machines that generate paper ballots with barcodes, which of course are not human readable and therefore subject to manipulation.

This is true even if the ballot shows in writing the candidates chosen because what the barcode says is what is counted.

The experts also called for risk-limiting audits of election results, regardless of how large the margin of victory.

Such audits are conducted by randomly doing a hand recount of paper ballots until a preset statistical measure of certainty is achieved when the reviewers can conclude the computer-tabulated election results reflect the actual votes cast.

“Elections are an American event,” Lankford observed. “They have partisan results, but the act of voting is an American event.”

“Election security should never be a partisan issue,” he went on to state.

“This is about the preservation of our democracy, and it’s something both parties — in fact independents, Republicans, Democrats, all parties — agree, that this should be a central issue for us.”

We are committed to truth and accuracy in all of our journalism. Read our editorial standards.