New American

Written by **William F. Jasper** on April 23, 2024

Published in the May 13, 2024 issue of the New American magazine. Vol. 40, No. 09

Voting Machine Warnings: Experts and Evidence

AP Images

Tech insecurity: The push for adopting voting machines was a fatally flawed idea from the beginning, and has endangered our elections.

Since the 2020 presidential election, Joe Biden, congressional Democrats, and their usual allies in the major media have relentlessly hammered as "baseless" every reasonable concern about the vulnerabilities of electronic voting machines and suspicions of voting-machine fraud. Don't listen to these wild "conspiracy theories," they tell us. The leading Fake News spigots (*The New York Times*, *The Washington Post*, CNN, NPR, MSNBC, and their imitators) have been especially vicious in attacking all who challenge our supposedly "safe and secure" digital voting systems. We can trust in the integrity of our voting systems, they assure us, because our federal and state authorities vouch for them!

However, this was not always the case. In elections since 2000, Democrats and the media sock puppets who now smear election challengers as "election deniers" and "MAGA extremists" were themselves leading critics of voting machines and warned of the dangers of hacking and fraud. Here are a few of their assertions and demands from the past that were then treated seriously by the same media that today dismiss similar warnings as "conspiracy theories":

• Representative Jerrold Nadler (D-N.Y.): "We are requesting an investigation into all the allegations, of irregularities with respect to the electronic and other voting machines so that people can have confidence in the result of this election, and so that any weaknesses are changed before the next election."

• Senator Kamala Harris (D-Calif): "There are a lot of states that are dealing with antiquated machines, right? Which are vulnerable to being hacked…. I actually held a demonstration for my colleagues here at the Capitol where we brought in folks who — before our eyes — hacked election machines, those that are being used in many states."

• Representative Adam Schiff (D- Calif.): "I continue to think that our voting machines are too vulnerable."

• Senator Ron Wyden (D-Ore.): "The biggest seller of voting machines is doing something that violates cybersecurity 101, directing that you install remote access software which would make a thing like that — you know — a magnet for fraudsters and hackers."

• Senator Amy Klobuchar (D-Minn.): "You could easily hack into [voting machines]. It makes it seem like all these states are doing different things, but, in fact, three companies are controlling [the elections]."

There are many similar quotes we could cite here, but you get the picture. Did the *Times*-CNN-MSNBC mob decry these politicians as wacko conspiracy theorists? You know the answer. In fact, readers might

recall that between 2002 and 2010 there was an ongoing bipartisan hullabaloo over the hacking scandals of the infamous and widely used Diebold Election Systems voting machines. Diebold and election officials adamantly insisted that everything was secure and no one need worry about tampering or hacking. However, multiple independent investigations by experts from Johns Hopkins University's Information Security Institute, RABA Technologies, Carnegie Mellon University, Princeton University, the state of California, the University of Iowa, and others found that the Diebold machines were riddled with "severe" security flaws that endangered elections.

And it wasn't only Diebold. A *New York Times* headline for December 15, 2007, read, "Ohio Elections Official Calls Machines Flawed." The opening sentence of the *Times* piece stated, "All five voting systems used in Ohio, a state whose electoral votes narrowly swung two elections toward President Bush, have critical flaws that could undermine the integrity of the 2008 general election, a report commissioned by the state's top elections official has found."

"It was worse than I anticipated," the official, Secretary of State Jennifer Brunner, said of the report. "I had hoped that perhaps one system would test superior to the others." Did the *Times* brand Brunner a "conspiracy theorist"? Of course not; she's a liberal-left Democrat. Besides, the study she cited credibly found that "voting machines and central servers made by Election Systems & Software; Premier Election Solutions, formerly Diebold; and Hart InterCivic; were easily corrupted."

Facing continuous lawsuits and cancellation of state contracts, Diebold rebranded itself as Premier Election Solutions and sold its voting software division to Election Systems & Software (ES&S), another of the big digital-voting-machine companies. ES&S, in turn, sold Premier (Diebold) to Dominion Voting Systems in 2010.

But, surely, the problems with Diebold were fixed by Diebold or its successors, right? Not even close. In fact, most of the reliable experts agree with *The New American* that electronic voting is *inherently* flawed and *cannot* be fixed. Digital voting is not secure, reliable, transparent, or verifiable.

As the following experts (and many others who could be cited) attest, the problems remain.

Dr. J. Alex Halderman

J. Alex Halderman (cse.engin.umich.edu)

Written by **William F. Jasper** on April 23, 2024

Published in the May 13, 2024 issue of the New American magazine. Vol. 40, No. 09

In January of this year, Dr. J. Alex Halderman was a star witness in a 12-day civil trial in the U.S. District Court for the Northern District of Georgia, before Judge Amy Totenberg. Halderman, a professor of electrical engineering and computer science at the University of Michigan and director of the university's Center for Computer Security and Society, is internationally famous as a voting-security specialist. He and his colleagues and students have repeatedly demonstrated, over the past two decades, how easily voting machines can be hacked and manipulated. Halderman is no MAGA Trumper; if anything, he appears to lean Democrat. He has often appeared as an expert witness before Congress and in lawsuits brought by "progressives," as was the case this year in Georgia, where the liberal-left Coalition for Good Governance was suing to prevent Georgia from using the Dominion voting machines.

Before Judge Totenberg and a packed court, Halderman demonstrated how easily anyone with knowledge and access could quickly overcome the supposed security of the Dominion voting machines. "During the second week of trial over the future of Georgia's election system," Law360 reported, "an expert on Thursday demonstrated how a $10 smart card, a USB drive or a pen can be used to install malware, change ballots and grant individuals 'super-user' access to the electronic in-person voting machines used by Georgians on election day."

Halderman began his demonstration by borrowing a pen from an attorney. Law360 describes what happened next:

> He inserted it into the back of a Dominion voting machine that was brought into the courtroom and held it there for a few seconds. This caused the machine to reboot into "safe mode," he said, explaining that allows users to access the machine's Android desktop.
>
> From there, Halderman explained that a user could copy, edit and change files on the voting machine, change its operating settings, install malware, and access what is known as a "terminal emulator." He then accessed the terminal emulator and entered a text command that would allow him to bypass the computer's normal security settings and obtain "super-user" access.
>
> According to Halderman, a person with super-user access would be able to read, monitor and change "anything" on the voting machine with "no limits." This includes ballots, he said. "All it takes is five seconds and a Bic pen," Halderman said.

But the professor was just getting started. He also showed how a $10 dollar smart card purchased online, such as those used by poll watchers, voters, and technicians, could be used to alter an election. Again from Law360:

> The poll worker and voter cards can be used county-wide to "print as many ballots as you would like," Halderman said. The technician card unlocks a menu through which he said software updates occur and ballot updates can be made, allowing anyone with the card to load data, update software and gain super-user access, he said….
>
> Halderman then used the machine to cast a ballot in a fake election between George Washington and Benedict Arnold. Though he voted for Washington, the printed ballot showed that he had voted for Arnold. That would, he said, be "undetectable" during an audit.

He went further, showing that once a USB flash drive was attached to the machine and malware installed, it was possible to flip votes. He cast five "Yes" votes on a printed ballot in an imaginary referendum. However, the optical scanner on the tabulator machine recorded it as two "Yes" votes and three "No" votes. These courtroom demonstrations were just examples of the many vulnerabilities that he detailed in a 96-page report he authored in 2021. Titled "Security Analysis of Georgia's ImageCast X Ballot Marking Devices," the Halderman study provides a chilling indictment of the claims that the voting machines used in our elections are safe and secure. Unfortunately, Halderman's report was sealed for two years by Judge Totenberg, a radical Obama appointee (and sister of left-wing NPR "journalist" Nina Totenberg). It was unsealed on June 14, 2023 and now can be accessed here.

"Georgia can eliminate or greatly mitigate these risks," says Halderman, "by adopting the same approach to voting that is practiced in most of the country: using hand-marked paper ballots and reserving BMDs [ballot-marking devices] for voters who need or request them."

Dr. Walter Daugherity

Walter Daugherity (tamu.edu)

Walter Daugherity is no newcomer to technology and cybersecurity. He received his doctorate in mathematics in 1977 from Harvard University, where he was awarded the Bowdoin Prize for outstanding writing. Daugherity is senior lecturer emeritus for the Department of Computer Science and Engineering at Texas A&M University and a computer consultant for major corporations and government agencies, including classified work. He is the author/co-author of numerous articles published in technical and science journals.

Daugherity served as an expert witness in the case brought before the U.S. Supreme Court by Arizona plaintiffs Kari Lake and Mark Finchem regarding their claims of election rigging in Arizona's November 2022 state elections, in which Lake ran for governor and Finchem ran for secretary of state. In his sworn declaration, Daugherity stated, "The evidence overwhelmingly demonstrates to a reasonable degree of scientific and mathematical certainty that the sequence of the Cast Vote Record ('CVR') data in both Maricopa County, Arizona, and Pima County, Arizona, shows artificial control over the tabulation of ballots and the election results for the November 2020 election."

"Such control could be implemented by manual means or by a computer algorithm, such as a

Proportional-Integral-Derivative ('PID') controller or some equivalent mathematical procedure," he said. However, effecting the thousands of observed deviations manually is not feasible. "This means," Daugherity asserts, "that some type of computer algorithm is indicated, and a PID controller is the simplest control function" that would produce the vote-result deviations seen in the election. "This same type of manipulation occurred both in Pima County, Arizona, which used ES&S voting machines (as did most other counties in Arizona), and also in Maricopa County, Arizona, which used Dominion voting machines (as did 23 other states), indicating that the same (or similar) software was responsible. Such manipulating software could be installed in a variety of ways, including vendor programming, operating system components, open-source or commercial off-the-shelf libraries, remote access, viruses or other malware, etc."

In his "Why Voting Computers Must Go" video posted on the Arkansas Voter Integrity Initiative Facebook page, Daugherity concludes his presentation by stating, "Voting machines cannot guarantee transparency, accuracy, or accountability, and therefore we need to return to hand-marked, hand-counted paper ballots."

Dr. Douglas Frank

Douglas Frank (The New American)

As we noted in our November 21, 2023 interview with him, Dr. Douglas Frank is a physicist, chemist, mathematician, author, inventor, science consultant, computer builder, teacher — and election expert. He has authored or co-authored 60 peer-reviewed articles in scientific journals. For the past couple of years, he has utilized his mathematical prowess and expertise in computer science to discover the sophisticated algorithms and techniques that are being used to manipulate our elections. He has traversed the country analyzing election results, investigating voter rolls, organizing voter-integrity activism, meeting with state and county officials, and testifying before legislatures. He has put his boots on the ground in 3,000 counties, appeared on countless TV and radio shows and podcasts, and addressed hundreds of local audiences.

According to Frank, the primary way elections are being stolen is through inflating the voter rolls and then using algorithms that add or subtract votes as needed as an election-tally process progresses. "The entire process is controlled, aided, and monitored by computer algorithms," he said in a Telegram

posting. "They've been developing these algorithms for years, and they are quite efficient. They also have the infrastructure and the resources to implement it." However, he notes, the voting machines themselves are also a major concern.

"So long as there's been elections, there's been cheating, including with paper ballots," he told *The New American*. "But the difference is whether it's localized and auditable and trackable and prosecutable or whether it's widespread and somebody living in Timbuktu can hack into your county and manipulate your election. You want to eliminate that possibility. Our elections are just too important. That's why I say 'Vote Amish' — all paper, no machines. Electronics just open you up to too many vulnerabilities. I build electronics for a living and I don't trust them. I write software for a living and I don't trust it. So anybody who is technically competent knows that electronics are the wrong way to do this. And there's really no way to ever secure it, because as soon as you think you have it secured, some clever person figures out a way to get into it."

Dr. Wenke Lee

Wenke Lee, Ph.D. is a professor of computer science and co-executive director of the Institute for Information Security & Privacy at the Georgia Institute of Technology. He has published nearly 150 cybersecurity research papers. "As part of a cybersecurity research community that works regularly with the Defense Department and global organizations," he says, "I am able to study many forms of cyberattack. New attacks are continuously discovered, while 'hardened systems' are proven to be flawed. This is why I remain an advocate for a hand-marked, paper ballot-based voting system, which guarantees that cyberattacks cannot alter votes."

Andrew W. Appel, Richard A. DeMillo, and Philip B. Stark

These are some of the big guns in computer science and technology security. In a 2019 paper entitled "Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters," Appel (Princeton), DeMil-lo (Georgia Tech), and Stark (University of California, Berkeley) argue that "election integrity requires a paper-ballot voting system in which, regardless of how they are initially counted, ballots can be recounted by hand to check whether election outcomes have been altered by buggy or hacked software." "A hacked BMD," they go on to note, "can print a vote on the paper ballot that differs from what the voter expressed or can omit a vote that the voter expressed."

Further, they write: "It is not easy to check whether BMD output accurately reflects how one voted in every contest.… Risk-limiting audits of a trustworthy paper trail can check whether errors in tabulating the votes as recorded altered election outcomes, but there is no way to check whether errors in how BMDs record expressed votes altered election outcomes. The outcomes of elections conducted on current BMDs therefore cannot be confirmed by audits.… To reduce the risk that computers undetectably alter election results by printing erroneous votes on the official paper audit trail, the use of BMDs should be limited to voters who require assistive technology to vote independently."

Most countries throughout the world still employ hand-marked, hand-counted paper ballots for their elections. What are these backward countries? Uganda, Zambia, Laos, Cambodia, or Bangladesh? No, try France, Germany, the U.K., Japan, Australia, Canada, Argentina, Spain, Sweden, Norway, Finland, the Netherlands, and many more economically and technologically advanced nations. They have listened to their own experts — and common sense. Some of them have already tried electronic voting and now reject it, usually due to well-founded security concerns based on their own experience. Paper

ballots work just fine for them, as they did previously for us. And they deliver faster, more accurate, less-contentious elections than we have been experiencing here in America since our legislators bought the Deep State techno-wizards' "brilliant" idea of digital elections. Along with Dr. Frank, we say "'Vote Amish' — all paper, no machines."

Written by **William F. Jasper** on April 23, 2024
Published in the May 13, 2024 issue of the New American magazine. Vol. 40, No. 09