Texas National Security Review: Volume 3, Issue 4 (Fall 2020)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

FIXING DEMOCRACY: THE ELECTION SECURITY CRISIS AND SOLUTIONS FOR MENDING IT

Kim Zetter

The 2000 presidential election debacle in Florida led to the widespread adoption of electronic voting machines in the United States. Yet these machines have proven to be more problematic than the punch card machines that precipitated Florida's crisis. Poorly built and poorly secured electronic voting machines have left U.S. elections vulnerable to software glitches and manipulation — by foreign adversaries or by malicious insiders — for 20 years. An easy solution exists to help restore integrity to the democratic process. But federal lawmakers have failed to act.

The targeting of voting infrastructure by Russian nation-state agents during the 2016 U.S. presidential election highlighted something computer security and election integrity experts had known for nearly two decades — that electronic voting systems used throughout the United States are vulnerable to manipulation from malicious outsiders and rogue insiders. Furthermore, the attempted interference in the 2016 election proved that little had been done to address this issue since the systems were first put in place in the early 2000s.

In 2016, amid growing concerns over the integrity of the voting process, election officials found themselves in the awkward position of having to assure the public that no one could hack the voting machines. Those machines, they argued, were never connected to the internet and therefore remained secure from external interference. Aside from the fact that this assertion was not true — some voting machines and backend systems that transmit and receive results on election night do connect to the internet and sometimes remain connected year-round — the statement exposed an alarming lack of awareness among those tasked with securing elections. Election officials appeared ignorant of the many ways voting systems can be hacked and election results manipulated even when those systems are not connected to the internet. Threats against voting machines that are not connected to the internet can come from malicious insiders who have physical access to the voting machines or to the systems that program those machines. Alternatively, external hackers can gain remote access to the networks of voting machine manufacturers and slip malicious code into the software and systems that those companies supply to states.[1]

With the heightened focus on election integrity, the Department of Homeland Security has been working with state and local election offices since 2016 to improve election security. But there is only so much they can do to address the problems, and the scope of their efforts is limited to election administration systems like voter registration databases. The voting systems responsible for casting and tallying votes still possess many of the same security vulnerabilities computer scientists found in them 20 years ago — vulnerabilities that would allow skilled actors to alter votes without leaving any trace. While the Department of Homeland Security can help election officials develop more secure handling of these machines, they cannot fix the security vulnerabilities inherent to them.

According to experts, there is little that individual states can do to mitigate the risks these machines pose before election day 2020 or future U.S. elections. The only way to address the problem is to mandate the use of voter-marked paper ballots and implement robust election audits. These audits can help verify the digital tallies or alert election officials when those results should not be trusted, based on evidence of potential interference.[2] Statisticians and election-security experts consider risk-limiting audits the gold standard. These are manual audits that compare digital votes against a percentage of paper ballots cast in every

1 Kim Zetter, "Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," *Vice/Motherboard*, Aug. 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.

2 Dan Webber, Harri Hursti, and Maggie Macalpine, "Getting Elections Right with Paper Ballots and Audits," *Government Technology*, Feb. 24, 2020, https://www.govtech.com/opinion/Getting-Elections-Right-with-Paper-Ballots-and-Audits-Contributed.html.

polling place in a county.[3] To implement such audits, states will have to amend their election laws. Currently, only three states have statutes requiring post-election risk-limiting audits.[4] In addition, election jurisdictions will have to revamp their procedures and train staff in how to conduct this type of election audit.

Instead of waiting for state legislatures to act, federal lawmakers could pass legislation mandating robust audits for federal elections. Some might see this as a more fitting solution to the problem since it was a federal election law — the Help America Vote Act, or HAVA — passed nearly 20 years ago that created the security and integrity problems the United States faces today. New federal legislation mandating election audits could help provide assurance that if the events of the 2016 presidential election were repeated, interference with voting machines or election results would be detected.

Helping America Vote

To understand the current election security crisis, we have to go back to the passage of HAVA in 2002.

It was May 2001, just six months after the U.S. Supreme Court intervened to halt the 2000 presidential election recount in Florida, allowing George W. Bush to claim victory in that state by a margin of fewer than 600 votes, thus securing the presidency. The debacle had been caused by "hanging chads" — paper ballots that threw the election result into question. Federal lawmakers in Washington, D.C., believed the antiquated paper punch cards used in Florida were the source of the problem and, in the aftermath of that controversial election, were determined to rid the nation of these systems and transition the United States to fully computerized elections using paperless, direct-recording electronic machines. Though computers were not new to U.S. elections — they had been used to tabulate votes cast on punch card machines and other equipment for three decades — fully computerized election machinery that used digital ballots instead of paper ones only accounted for about 9 percent of U.S. voting machines in 2002.[5] In the spring of 2001, federal officials were contemplating passing a bill that would give states federal money — around $4 billion — to make the switch.

But Rebecca Mercuri, a computer scientist at Bryn Mawr College, hoped to dissuade them. Mercuri had been railing against paperless voting machines for more than a decade. In 1989, her Pennsylvania county had contemplated buying new, paperless voting machines, and Mercuri had convinced officials to drop the plan. Now she was set to testify on paperless voting before the House Committee on Science. Mercuri was confident federal lawmakers would listen to her once she described the myriad security problems with the machines and how they made it impossible to audit election results.[6]

During her testimony, Mercuri spoke bluntly. "Fully electronic systems do not allow the voter to independently verify that the ballot cast corresponds to that one that was actually recorded, transmitted or tabulated," she told the panel. Anyone — a rogue programmer working for one of the voting machine vendors, an election worker with access to the machines, a hacker able to get into the systems, even one of her own students — could write code that would cause the systems to display one thing on-screen to voters while recording something entirely different on their memory cards. And with no paper backup ballots to audit the digital tally and verify the results, there would be no way for anyone to know it had occurred, she said.[7]

Two other experts at the hearing added to Mercuri's concerns. They warned the lawmakers that the electronic voting machines currently available on the market had been designed in the 1980s, when computer security was an undeveloped discipline. The standards by which the systems were tested and certified included few cyber security measures. The machines, one of the experts noted, had software bugs and security vulnerabilities that made them unsuitable for their critical role in ensuring smooth democratic processes. He advised the lawmakers to hold off on giving states money to purchase more of the flawed machines until the standards could be rewritten and more secure machines could be developed.[8]

There was plenty of evidence to support the

3 Christopher Deluzio, "A Smart and Effective Way to Safeguard Elections," *Brennan Center for Justice*, July 25, 2018, https://www.brennancenter.org/our-work/analysis-opinion/smart-and-effective-way-safeguard-elections.

4 National Conference of State Legislatures, "Risk-Limiting Audits," Feb. 17, 2020, https://www.ncsl.org/research/elections-and-campaigns/risk-limiting-audits.aspx.

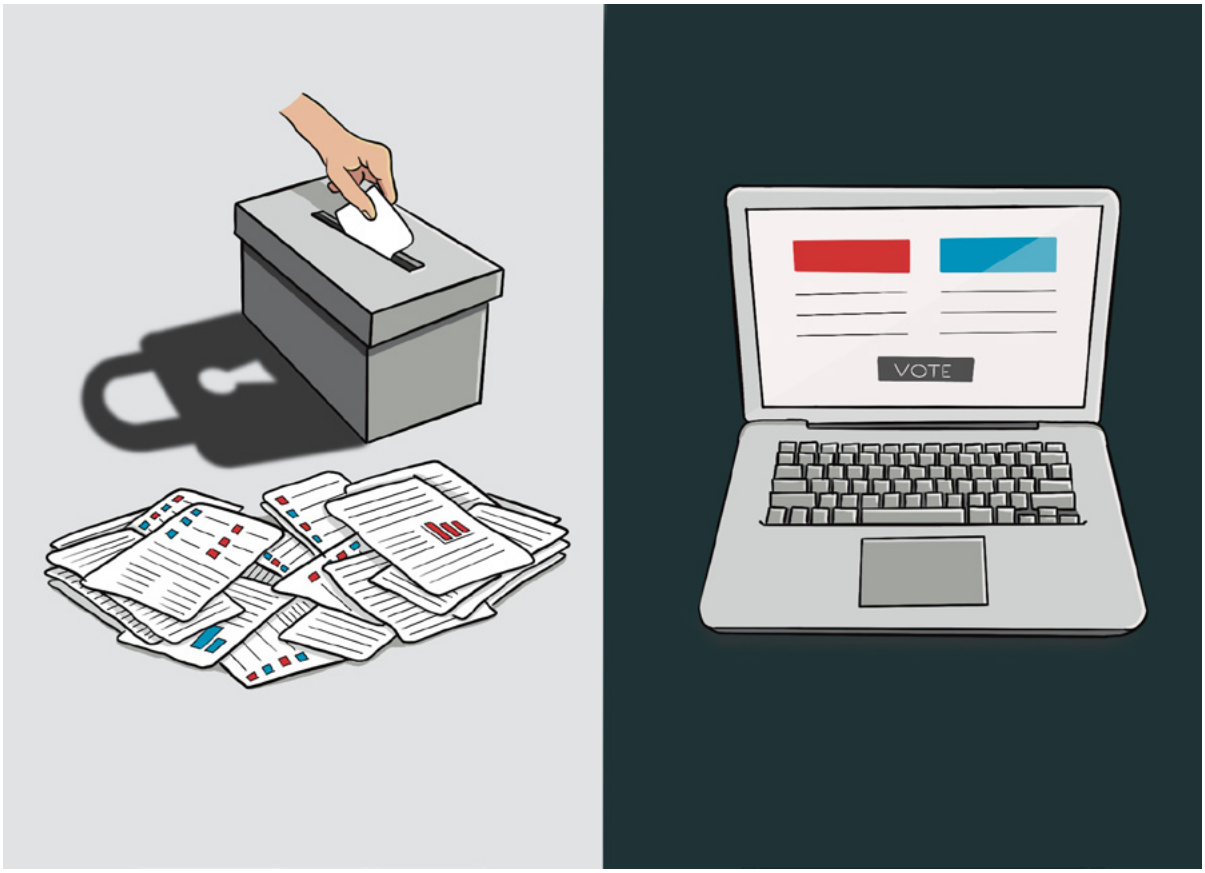
5 *Improving Voting Technologies: The Role of Standards* (Washington, DC: Committee on Science, 2001), 166, http://commdocs.house.gov/committees/science/hsy73327.000/hsy73327_0.htm#166.

6 Juliana Rosati, "Rebecca Mercuri: BMC's Electronic Voting Expert," *The College News*, March 7, 2001, http://www.notablesoftware.com/Press/BMCmerc.html.

7 *Improving Voting Technologies*, 31.

8 *Improving Voting Technologies*, testimony of Roy G. Saltman, 34-38, and Douglas W. Jones, 38-41.

THERE WAS PLENTY OF EVIDENCE TO SUPPORT THE EXPERTS' ASSERTION THAT ELECTION COMPUTERS WERE NOT READY FOR WIDESPREAD USE.



experts' assertion that election computers were not ready for widespread use. In 1985, for example, an Indiana lawyer filed a federal lawsuit over vote-counting software created by Computer Election Systems. Other plaintiffs in West Virginia, Maryland, and Florida filed similar suits against the company. Computer experts hired by the plaintiffs said the company's program was open to outside interference — they argued that anyone could hack the software and alter vote totals without leaving a trace of their deed. The tabulation code used to count more than one-third of the votes in the presidential race in 1984, they warned, was vulnerable to manipulation and fraud. Furthermore, the experts argued that log files intended to track changes made to the program could be altered to hide malicious activity.[9]

In numerous instances before 2002, mishaps involving electronic voting underscored the need for paper backups. In 1971, a computer counting punch card ballots in Ohio misallocated votes due to a programming error. This error was correctable only because the paper punch cards could be recounted.[10] In 2000, a malfunctioning optical-scan voting machine in Iowa erroneously calculated 4 million votes in a race, though only 300 ballots were scanned. Optical-scan machines read paper ballots hand-marked by voters. In this case, as in Ohio, election officials arrived at the correct tallies by recounting the paper ballots. Finally, as lawmakers were preparing to vote on HAVA in 2002, two Republican commissioners in Texas won races by unexpectedly large margins, raising suspicions of irregularities in the vote-counting. When election officials manually recounted the optical-scan ballots, Democratic candidates won in both races.[11]

These incidents should have convinced federal lawmakers in 2002 that paper ballots were critical to providing trust in the legitimacy of election outcomes. Nevertheless, lawmakers appeared to ignore the warnings. Rep. Steny Hoyer, one of the authors of HAVA, said recently that he never heard about

9 David Burnham, "Computerized Systems for Voting Seen as Vulnerable to Tampering," *New York Times*, July 29, 1985, https://www.nytimes.com/1985/07/29/us/computerized-systems-for-voting-seen-as-vulnerable-to-tampering.html.

10 Institute of Election Administration, American University and National Scientific Corporation, *A Study of Election Difficulties in Representative American Jurisdictions* (Washington, DC: American University, 1973), 1-10.

11 Jim Carlton, Chip Cummins, Patricia Callahan, and Anne Marie Squeo, "Fuzzy Numbers: Election Snafus Went Far Beyond Florida in Year When It Mattered," *Wall Street Journal*, Nov. 17, 2000, https://www.wsj.com/articles/SB974424706937213629; "Ballot Glitches Reverse Two Election Results," *Houston Chronicle*, Nov. 8, 2002.

any security problems with the machines when they were debating the bill. At the time, he believed they were improving elections with the legislation.[12]

Hoyer and his colleagues also missed another significant consequence of their legislation: HAVA undermined one of the most important gains of earlier voting rights legislation — the right of election observers to watch vote-tallying procedures after an election to ensure a transparent count and provide confidence in the results. The electronic machines put in place after HAVA was passed in 2002 were proprietary black boxes with software protected by trade secrets. The use of these machines made the vote-counting process unobservable. Rather than improving election integrity, electronic voting machines produced more problems than the controversial punch card machines they replaced — problems that persist today.

Ironically, analysis of the 2000 election completed before the passage of HAVA in 2002 concluded that many of the problems in Florida were due to a poorly designed ballot that confused voters, card stock that made it difficult to punch the ballots properly, and other issues that could not be addressed by introducing electronic voting.[13] One study from researchers at the Massachusetts Institute of Technology and Caltech concluded that many of the problems could be solved by replacing the punch card machines with optical-scan machines, where voters use a pencil or pen to mark a paper ballot.[14] But federal lawmakers arrived at a different conclusion. "The lesson that [lawmakers] derived from Florida [in] 2000 was that paper is bad because of hanging chads. The lesson should have been 'badly-engineered paper is bad,' not that paper is bad," says Barbara Simons, past president of the Association for Computing Machinery and current member of the board of directors for Verified Voting, an election integrity group.[15]

In 2018, Hoyer admitted that he and his colleagues had missed the security and auditability problems with electronic voting machines. "[W]e were focused more on getting [rid of] a technology that had failed miserably in 2000," he said. "There was a perhaps misplaced confidence that the technologies that would be adopted by locals would be accurate and would be, in effect, much less subject to mistake or manipulation [than punch card machines]."[16]

In the decade after HAVA, as paperless machines broke down during elections, lost digital ballots, produced faulty results, and proved vulnerable to hacks (based on assessments by computer security experts who examined their software), California, Florida, Ohio, and other states came to realize the folly of purchasing paperless voting machines and switched to optical-scan machines that could be audited. California, for example, mandated in 2003 that all counties had to use either optical-scan machines or paperless direct-recording electronic machines outfitted with printers to produce a paper backup, similar to a cash register receipt, of the digital ballots. When voters mark their choices on-screen, the system prints the choices on a scrolling receipt that remains behind a glass partition. Voters are supposed to check the receipt to verify the ballot before pressing a button that sends it to the ballot box. The problem with a paper trail that is printed by the machine and not hand-marked by the voter is that the machine can be manipulated to show voters their correct votes on the paper receipt while recording different votes on the machine's memory card. Thus, the machine is still vulnerable to interference or malfunctions without a voter-marked paper ballot audit to confirm the result of the election.

California mandated paper ballots and paper backup receipts after discovering that Diebold Election Systems, one of the leading manufacturers of electronic voting machines at the time, had secretly installed software updates on machines without informing officials, in violation of state law.[17] The paper ballots, lawmakers hoped, would provide a way to trust election results even if the integrity of election vendors and their machines could not be trusted. Most other states eventually followed California's lead, including Florida, which mandated paper ballots or voting machine printers statewide in 2006. It did so after a controversial election in which 18,000 ballots cast on paperless, direct-recording electronic machines showed no votes cast in a race in the 13th congressional district, though voters completed other races on the ballot. Election officials insisted that voters had intended to leave that race blank. Without voter-marked paper ballots to audit the digital tally and prove otherwise, the Re-

12 Author interview, Aug. 1, 2018.

13 "Newspaper: Butterfly Ballot Cost Gore White House," *CNN*, March 11, 2001, https://www.cnn.com/2001/ALLPOLITICS/03/11/palmbeach.recount/.

14 Katharine Q. Seelye, "Study Says 2000 Election Missed a Million Votes," *New York Times*, July 17, 2001, https://www.nytimes.com/2001/07/17/us/study-says-2000-election-missed-millions-of-votes.html.

15 Author interview, July 17, 2018.

16 Author interview, July 17, 2018.

17 Kim Zetter, "E-Votes Must Leave a Paper Trail," *Wired*, Nov. 21, 2003, https://www.wired.com/2003/11/e-votes-must-leave-a-paper-trail/.

publican candidate won by fewer than 400 votes.[18]

Oddly, one state that experienced the same problems that Florida and California experienced opted not to replace its paperless machines: Georgia. In 2002, Diebold reportedly installed uncertified software on all of Georgia's paperless machines, as it had done in California. Georgia retained its machines despite this development.[19] In 2018, in the lieutenant governor's race between GOP candidate Geoff Duncan and Democrat Sarah Riggs Amico, 160,000 ballots showed no vote cast in that contest — a statistically anomalous event. Georgia officials denied the machines were at fault.[20] Officials did finally replace the paperless machines in 2020, however, after state lawmakers passed a bill allocating funding to purchase new machines and a federal judge barred the state from using its old machines after 2019.[21]

...THOUGH SOME STATES DO CONDUCT AUDITS, THEY ARE FREQUENTLY LIMITED IN SCOPE. ... IN ADDITION, NOT ALL AUDITS INCLUDE ABSENTEE BALLOTS MAILED IN BY VOTERS AND FED INTO AN OPTICAL-SCAN MACHINE IN THE COUNTY ELECTION OFFICE...

But even with these changes, 20 years later the legacy of HAVA stubbornly lives on. Louisiana still uses paperless, direct-recording electronic machines statewide. Seven other states have one or more counties that use them as well.[22] Many other states have modified these machines with printers to produce a "voter-verifiable" paper trail, but as noted, this does not have the same integrity as optical-scan systems. It would be a mistake, however, to believe that optical-scan machines alone are the answer for improving election integrity.

Optical-Scan Machines: An Imperfect Solution

Although optical-scan machines are considered a better alternative to direct-recording electronic machines, they are not a panacea for America's current voting security issues. Their software is vulnerable to hacks and they can malfunction like any other computer.

In 2008 in California, an optical-scan system made by Diebold Election Systems inexplicably dropped a batch of 197 absentee ballots from memory. The county caught the problem only because it had launched a unique ballot transparency project that year — in addition to scanning ballots through its Diebold scanner, the county purchased an off-the-shelf Fujitsu scanner and scanned the paper ballots a second time through that machine. When officials noticed that the total number of ballots scanned on the two machines were different, they discovered that 197 ballots scanned into the Diebold system on election day had subsequently disappeared from the system. When officials examined the system's activity log, there was no record that the ballots were ever in the system, though they had shown up in vote tallies during the initial days after the election. California officials were never able to fully determine what had gone wrong.[23]

But there is another reason optical-scan machines are not a cure-all for the problems afflicting electronic voting. Unless election officials do a robust post-election audit of the paper ballots to compare them against the digital ballots stored in an optical-scan machine's memory, the paper ballots are pointless. Though some states do conduct audits, they are frequently limited in scope. In many cases, county election officials randomly choose 1 percent of precincts and manually audit only ballots cast in those polling places. If a problem occurred in any precinct not included in that random 1 percent draw, it would remain undetected. In addition, not all audits include absentee ballots mailed in by voters and fed into an optical-scan machine in the county election office. This is a sig-

18 Kim Zetter, "Docs Point to E-Voting Bug in Contested Race," *Wired*, April 17, 2007, https://www.wired.com/2007/04/docs-point-to-e-voting-bug-in-contested-race/.

19 Kim Zetter, "Did E-Vote Firm Patch Election?" *Wired*, Oct. 13, 2003, https://www.wired.com/2003/10/did-e-vote-firm-patch-election/; Neena Satija, Amy Gardner, and Joseph Marks, "As Georgia Rolls Out New Voting Machines for 2020, Worries About Election Security Persist," *Washington Post*, Dec. 23, 2019, https://www.washingtonpost.com/politics/as-georgia-rolls-out-new-voting-machines-for-2020-worries-about-election-security-persist/2019/12/23/c5036d74-2017-11ea-bed5-880264cc91a9_story.html.

20 Kim Zetter, "Georgia Voting Irregularities Raise More Troubling Questions About the State's Elections," *Politico*, Feb. 12, 2019, https://www.politico.com/story/2019/02/12/georgia-voting-states-elections-1162134.

21 Stephen Fowler, "Judge Says Georgia Must Scrap Outdated Electronic Voting Machines After 2019," *NPR*, Aug. 15, 2019, https://www.npr.org/2019/08/15/751419405/judge-denies-request-to-scrap-georgias-outdated-electronic-voting-machines-for-2.

22 "Verifier," *Verified Voting*, n.d., https://www.verifiedvoting.org/verifier/.

23 Kim Zetter, "Serious Error in Diebold Voting Software Caused Lost Ballots in California County," *Wired*, Dec. 8, 2008, https://www.wired.com/2008/12/unique-election/.

nificant oversight, as the number of absentee ballots cast by voters has greatly expanded in recent years: At least 24 percent of voters cast absentee ballots in the 2016 election.[24] More are expected to cast absentee ballots in the 2020 presidential election due to the health risks posed by the novel coronavirus and in-person voting. Experts anticipate that voters will cast more than 80 million ballots by mail this year, more than double the number cast in 2016.[25]

Election integrity activists and federal lawmakers like Sen. Ron Wyden (D-OR) and Sen. Elizabeth Warren (D-MA) have pushed federal legislation that would require voter-marked paper ballots and risk-limiting audits in every jurisdiction.[26] However, these efforts have been unsuccessful. As it stands, optical-scan voting machines offer only a partial solution to election security issues without robust audits.

Many states have begun to purchase a hybrid type of voting system that uses a ballot-marking device with a touch screen, and an optical scanner to record the votes. This system provides the accessibility of a touch screen for disabled voters along with the auditability of a paper ballot. Voters mark their choices on the touch screen, and the system prints out a ballot, which is then scanned through the optical-scan machine. The problem with a ballot-marking device, however, is that a computer marks the paper, not the voter. Unless voters review their ballots after they are printed and before they are scanned, the system could show them one set of votes on-screen and record something else on the ballots. Some ballots also include a quick-response (QR) code or bar code on the printed ballot. If the optical scanner is allowed to scan the code instead of the human-readable portion of the ballot, the system could be manipulated to record votes differently in the QR code than on the human-readable portion that voters can review.

If We Bank Online, Why Can't We Vote Online?

Despite the lessons learned from paperless voting over the last two decades, West Virginia, Delaware, and other states have considered adopting internet voting in various forms in recent years.[27] Internet voting can involve filling out and casting ballots on a computer or mobile phone or receiving ballots electronically, printing them, and filling them out on paper before returning them as an image file via email, fax, or direct upload to a server.

In May 2020, the Department of Homeland Security issued guidelines to election officials around the country informing them that electronic ballot return is a "high-risk" endeavor that would allow votes to be manipulated on a large scale.[28] But 23 states already offer this option for military and civilian voters who are out of the country and for whom absentee ballots sent through the U.S. Postal Service might not arrive to election offices in time.[29] Currently, only a small percentage of voters return their ballots electronically, but in 2020, that number could explode if states decide to offer voting by mail to anyone who wishes to vote this way due to health concerns around in-person voting during the novel coronavirus pandemic. This would place a significant burden on election officials and the U.S. Postal Service to process millions of mail-in ballots by election day, something that has long been a growing problem even without the additional challenges introduced by the virus.[30] The expansion in voting by mail coupled with postal problems could push states to allow more voters to return their ballots electronically.[31]

None of the 50 states and territories have adopted full-on internet voting — where voters make their selections and cast their ballots through an online interface — though there has been pressure to move in that direction. The novel coronavirus is adding to that pressure. As people become used to doing more things remotely during the pandemic — work-

24 Election Assistance Commission, "EAVS Deep Dive: Early, Absentee and Mail Voting," *EAC*, Oct. 17, 2017, https://www.eac.gov/documents/2017/10/17/eavs-deep-dive-early-absentee-and-mail-voting-data-statutory-overview.

25 Juliette Love, Matt Stevens, and Lazaro Gamio, "Where Americans Can Vote by Mail in the 2020 Elections," *New York Times*, Aug. 14, 2020, https://www.nytimes.com/interactive/2020/08/11/us/politics/vote-by-mail-us-states.html.

26 "Wyden, Gillibrand, Markey, Merkley, Murray and Warren Introduce Bill to Secure Elections," *Ron Wyden*, June 12, 2018, https://www.wyden.senate.gov/news/press-releases/wyden-gillibrand-markey-merkley-murray-and-warren-introduce-bill-to-secure-elections-.

27 Eric Geller, "Some States Have Embraced Online Voting. It's a Huge Risk," *Politico*, June 8, 2020, https://www.politico.com/news/2020/06/08/online-voting-304013.

28 *Mail-In Voting in 2020 Infrastructure Risk Assessment* (Rosslyn, VA: Cybersecurity and Infrastructure Security Agency, 2020), https://www.cisa.gov/sites/default/files/publications/cisa-mail-in-voting-infrastructure-risk-assessment_508.pdf.

29 National Conference of State Legislators, "Electronic Transmission of Ballots," *NCSL*, Sept. 5, 2019, https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx.

30 Ryan McCarty and Maryam Jameel, "The Postal Service Is Steadily Getting Worse — Can It Handle a National Mail-In Election?" *ProPublica*, June 15, 2020, https://www.propublica.org/article/the-postal-service-is-steadily-getting-worse-can-it-handle-a-national-mail-in-election.

31 Kim Zetter, "US Government Plans to Urge States to Resist 'High-Risk' Internet Voting," *The Guardian*, May 8, 2020, https://www.theguardian.com/us-news/2020/may/08/us-government-internet-voting-department-of-homeland-security.

ing, teaching, psychotherapy — it will be harder to convince them to give up that convenience when it comes to voting, even after the pandemic has passed.

Proponents of internet voting argue that it is a viable option now that so many everyday activities have moved online.[32] If the internet is safe enough for banking, why isn't it safe for voting? But this is a false equivalency. Banking and voting differ in significant ways. With banking, customers do not conduct transactions anonymously. Moreover, there is a record of every transaction. If there is suspicious activity, customers can see it on a bank statement or in their account balance and have an opportunity to rectify errors or fraud. In most cases, the customer will suffer no liability; the bank will restore stolen money. But voting is conducted anonymously by law in the United States; if votes are altered — either on the voter's personal device before the ballot is sent or on the government server that receives the ballot — there is no way to go back to voters to determine the votes they intended to cast.[33] Similarly, there is no foolproof way for voters to check that their votes were recorded correctly and not altered either by a glitch in the tabulation software or a hacker. There is an additional risk with online voting: Hackers could disenfranchise voters by launching denial-of-service attacks against the county servers set up to receive votes over the internet, prevent voters' ballots from reaching their destination, or intercept and delete ballots during transmission.

No one has produced an online voting system that is sufficiently secure. In the United States, several jurisdictions have piloted a mobile phone voting application called Voatz. But that system was recently shown to have serious security issues by experts who examined it.[34] As for online voting done through an interface, systems rolled out in Estonia, Australia, and Switzerland have all had security issues, some of them severe.[35] Computer security experts say that there may come a time in the future when computer security technologies and techniques advance to the point that internet voting becomes safe and secure. But now is not that time, nor will such a time arrive in the foreseeable future.[36]

These are just a few of the issues plaguing the current state of election security in the United States. There are many others not covered here: poor testing and certification procedures that have allowed badly designed systems to be sold to states, the lack of oversight and transparency around voting-machine vendors and their code to ensure that the systems do what the vendors say they do and do not have backdoors that the vendors or others can use to get into voting systems, and the absence of a nationwide system to track problems with voting machines when they occur in elections to understand the scope of issues.

In 2001, lawmakers who supported HAVA optimistically believed that the country would overcome the 2000 election debacle with passage of the legislation. "One year ago tonight, in Bush v. Gore, the United States Supreme Court effectively determined the outcome of our last Presidential election," Hoyer said during a House debate on the bill. "But today this House has an historic opportunity to let this day be remembered not for one of the most controversial decisions in the Court's history, but for congressional action to protect our most cherished democratic right: the right to vote and the right to have that vote counted."[37] Yet the ambitions of HAVA have mostly gone unrealized. Twenty years later, as Russian hackers stand ready to once again interfere with a U.S. presidential election — and with the rising threat from other state actors, including China and Iran — the right

32 Geller, "Some States Have Embraced Online Voting."

33 Ronald L. Rivest, *Electronic Voting* (Cambridge, MA: Laboratory for Computer Science, Massachusetts Institute of Technology, n.d.), https://people.csail.mit.edu/rivest/Rivest-ElectronicVoting.pdf.

34 Dan Guido, "Our Full Report on the Voatz Mobile Voting Platform," *Trail of Bits*, March 13, 2020, https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/; Michael Specter, James Koppel, and Daniel Weitzner, "FAQ on the Security Analysis of Voatz," *Internet Policy Research Initiative*, Feb. 14, 2020, https://internetpolicy.mit.edu/faq-on-the-security-analysis-of-voatz/.

35 For Estonia, see, Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman, "Security Analysis of the Estonian Internet Voting System," *Proc. 21st ACM Conference on Computer and Communications Security* (November 2014), https://jhalderm.com/pub/papers/ivoting-ccs14.pdf; for Australia, see, J. Alex Halderman and Vanessa Teague, "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election," *Cornell University*, April 22, 2015, https://arxiv.org/abs/1504.05646; for Switzerland, see, Kim Zetter, "Experts Find Serious Problems with Switzerland's Online Voting System Before Public Penetration Test Even Begins," *Vice/Motherboard*, Feb. 23, 2019, https://www.vice.com/en_us/article/vbwz94/experts-find-serious-problems-with-switzerlands-online-voting-system-before-public-penetration-test-even-begins; see also, Kim Zetter, "Researchers Find Critical Backdoor in Swiss Online Voting System," *Vice/Motherboard*, March 12, 2019, https://www.vice.com/en_us/article/zmakk3/researchers-find-critical-backdoor-in-swiss-online-voting-system.

36 American Association for the Advancement of Science, "Internet or Online Voting Remains Insecure," *AAAS*, n.d., https://www.aaas.org/programs/epi-center/internet-online-voting#NIST.

37 Neil Volz, *Into the Sun: A Memoir* (Bloomington, IN: AuthorHouse, 2011), 114-115.

for voters to have their vote counted, and counted accurately, remains at risk.[38]

Audits Are the Answer

What can officials do to inject integrity into elections? And how can they reassure the public that announced tallies accurately represent the will of voters and not the malign influence of hackers or external agents?

Computer security and election integrity experts agree that the best way to address the problems in election software is to implement a solution that is software-independent. The clearest solution lies with paper ballots and post-election audits.

This isn't about removing computers and software from elections. Computers offer many advantages in elections — they can tally results quickly, they are better able to handle the lengthy and complex ballots used in U.S. elections, and they can count ballots with more accuracy than human election officials.[39] Rather than remove computers from the election process, an effective solution to the problem of election security would combine the latest technology with methods that ensure an accurate and verifiable tally — that is, with paper ballots and risk-limiting audits. This solution would provide some transparency in an inherently opaque process in order to restore trust in election outcomes.

The first step, experts say, would be federal legislation mandating all voting machines use a voter-marked paper ballot. This would force election jurisdictions that still use paperless systems to replace those systems with a voting system or process that uses a full-size paper ballot.[40] That legislation would also need to require election jurisdictions to implement mandatory post-election risk-limiting audits designed to detect mistakes related to the voting machines or tabulation software.[41] If no discrepancy arises between the original digital tally and the audited paper ballots, election officials can provide the audited tallies as evidence should anyone challenge the election outcome.

But federal legislation mandating paper ballots and audits will not be enough. State election laws will have to be amended as well. Should an audit show a discrepancy between the digital tally and the audited paper ballots, it will fall on state election laws to determine whether the paper or electronic ballots should prevail as the official ballots of record. If for some reason both paper and electronic ballots become suspect, state election laws will need to determine whether the election should be repeated.

Conclusion

The good news is that experts have already spent a lot of time and effort developing this auditing process. The bad news is that the United States is still a long way from having those solutions in place. Vulnerabilities within U.S. election systems have made it possible for electoral processes to be upended by technical malfunctions or foreign interference. Until action is taken to ensure the integrity of results, the elections that form the cornerstone of democracy will always be vulnerable to dispute, further eroding confidence in the domestic political process.

Kim Zetter *is an award-winning investigative journalist who has covered cyber security and national security for more than a decade, with a special focus on election security and cyber warfare. She has covered election security extensively for* Wired *and* Politico *and wrote a* New York Times Magazine *cover story on the topic in 2018. She is also the author of the book* Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, which tells the true story of a covert digital attack launched by the United States and Israel against Iran's nuclear program.*

Photo: Joebeone at the English language Wikipedia / CC BY 2.5 (https://creativecommons.org/licenses/by/2.5)

38 Office of the Director of National Intelligence, "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," *DNI*, Aug. 7, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

39 Stephen Ansolabehere and Andrew Reeves, *Using Recounts to Measure the Accuracy of Vote Tabulations: Evidence from New Hampshire Elections 1946-2002* (Cambridge, MA: Caltech-MIT Voting Project, 2004), https://dspace.mit.edu/bitstream/handle/1721.1/96548/vtp_wp11.pdf.

40 Patrick Howell O'Neill, "16 Million Americans Will Vote on Hackable Paperless Machines," *MIT Technology Review*, Aug. 13, 2019, https://www.technologyreview.com/2019/08/13/238715/16-million-americans-will-vote-on-hackable-paperless-voting-machines/.

41 Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology, *Securing the Vote: Protecting American Democracy* (Washington, D.C.: National Academies Press, 2018), 101, https://www.nap.edu/read/25120/chapter/7#95.