Electronic Voting Is a Threat to the Constitution

by Edward Spannaus

In the wake of widespread irregularities in the Jan. 13 Washington, D.C. primary, Democratic presidential candidate Lyndon LaRouche gave his endorsement to the calls by local officials for an investigation of the vote tabulation in the primary election (See *EIR,* Jan. 23). Moreover, LaRouche has emphasized the threat to the fundamental constitutional right of the citizen to vote, and to the right to a fair election, which is posed by the introduction of new computerized vote-counting systems—systems which are easily rigged, and which render it impossible to verify the vote count.

In a Jan. 18 editorial, the *New York Times* issued the following warning: "The morning after the 2000 election, Americans woke up to a disturbing realization: our electoral system was too flawed to say with certainty who had won. Three years later, things may actually be worse. If this year's Presidential election is at all close, there is every reason to believe that there will be another national trauma over who the rightful winner is, this time compounded by troubling new questions about the reliability of electronic voting machines."

It's a lot worse than the *New York Times* is admitting. As a result of the Help America Vote Act (HAVA), passed by the Republican-controlled Congress in 2002, the Federal government is now subsidizing and encouraging the adoption of insecure electronic voting systems by the states. Under the pretext of assisting persons with disabilities, by 2006 every polling place used in a Federal election is required to have at least one direct recording electronic (DRE) device, or another device "equipped for individuals with disabilities."

The only good news, is that a study issued on Jan. 22 by the Election Reform Information Project and electionline.org, shows that these "reforms" are proceeding more slowly than anticipated, explaining that "those who expected all the ills revealed in the 2000 elections to be cured by November 2004 will certainly be surprised." They don't admit, that in this case, the cure is worse then the disease.

The study does attribute some of the delays to security concerns, reporting: "Debates over the accuracy, security and integrity of paperless, electronic voting continue to delay and in some cases alter machine replacement plans in a number of states."

The study also complains: "Once the darlings of election reform, direct-recording electronic (DRE) machines, using touch-screen or scrolling-wheel models, have raised more suspicion than the antiquated punch-card and lever machines they were slated to replace. The absence of voter-verified paper trails has computer scientists, members of Congress and newspaper editorial boards concerned."

Another problem: "In a closely-related issue, the constant backlash against electronic voting might have sapped voter confidence in the same way the Florida fiasco and the problems with punch cards, vague recount rules, and poorly designed ballots did in 2000." The report laments that "HAVA was passed, its supporters said, largely to restore shaken faith in America's voting system," but has it succeeded?

Another survey shows that nationwide, 56% of voters will use touch-screen or optical scanning systems this year, up from 43% in 2000. Punch cards are still in use in 22 states. Only Georgia and Maryland have made a complete cut-over to touch-screen systems, despite doubts about their security.

The Georgia 'Upset'

Many questions and suspicions have been raised about the 2002 elections in Georgia, its first election using Diebold touch-screen machines statewide—indeed, the first election in the country conducted solely on touch-screen devices. The election produced a Republican sweep which raised a lot of

eyebrows. For example, incumbent Democratic Senator Max Cleland was leading Rep. Saxby Chambliss 49-44% in polls before the elections, but Chambliss won by 53-46%. Another unexpected upset was in the Governor's race, where a Democratic pre-election lead of 48-39% was reversed in a 52-45% Republican victory, the first Republican elected Governor of Georgia in 135 years. Such things do happen, of course, and the first explanation offered was a voting surge by angry white males triggered by the abolition of the Confederate flag as the state banner. However, post-election demographic analysis showed no such surge; the only population sector showing an increase in turnout was black women.

Fueling suspicions were many irregularities: machines freezing up, memory cards missing and lost.

Moreover, Georgia's election was not run by state officials; it was conducted by a private company, under a strict trade-secrecy contract that prohibited election officials from doing anything to the equipment, or examining the software to see if the systems were operating correctly.

Of course none of this proves that fraud, or even accidental mistabulation of the vote, actually occurred. But, the problem is that no one can prove that it *didn't.* There is no way of knowing, since there is no way of conducting even a partial recount. "Trust me," says Diebold—and the voters have no choice.

It doesn't help that Diebold has extensive ties into Republican circles, and that its chief executive, Wally O'Dell, is a frequent visitor to the Bush ranch in Crawford, Texas; that he hosted a $600,000 fundraiser for Dick Cheney; or that he sent out a fundraising letter declaring that he was "committed to helping Ohio to deliver its electoral votes to the President next year"—even as his Ohio-based company was bidding for the state's contract for new voting machines.

"Trust me," says Wally O'Dell—and you, the voter, have no choice, for his machines produce no paper trail, no audit trail, and provide no ability to conduct a recount.

Security Flaws and Vulnerabilities

Experts who have analyzed the new generation of electronic voting systems have emphasized that there is simply no way to be certain that the vote is being counted accurately.

- The most cautious study on DRE systems, done by the Congressional Research Service (CRS) and issued in November 2003, concluded that "at least some current DRE's clearly exhibit security vulnerabilities."

The study reports that "the more complex a piece of software is, the more vulnerable it is to attack," and continues: "That is because more complex code will have more places that malware can be hidden, and more potential vulnerabilities that could be exploited, and it is more difficult to analyze for security problems. In fact, attackers often discover and exploit vulnerabilities that were unknown to the developer, and many experts argue that it is impossible to anticipate all possible weaknesses and points of attack for complex software."

Touch-screen voting on a direct-recording electronic machine.

"The ballot itself consists of redundant electronic records in the machine's computer memory banks, which the voter cannot see," says the report.

The CRS report acknowledges that "voters must have confidence in the integrity of the voting systems they use if they are to trust the outcomes of elections and the legitimacy of governments formed as a result of them," and it adds: "If the concerns that have been raised about DRE security become widespread, that confidence could be eroded, whether or not those concerns are well-founded."

But the CRS report acknowledges, with respect to what is probably the most basic means of ensuring confidence in voting results—recounting the vote—that "problems with the machines themselves, including tampering, would probably not be discovered through a recount."

The Diebold Study

- A study of Diebold DRE machines by computer scientists from Johns Hopkins and Rice Universities, was released on July 23, 2003. This study was based on a review of Diebold software source code which had been inadvertently placed by Diebold on a public Internet site. Diebold has admitted that the software code on which the study is based is authentic, and that the study's conclusions regarding the software are essentially correct, but they claim that other factors will protect elections against their software.

The Hopkins study found "stunning flaws," including flaws that would allow a hacker to break into the system and alter the program, and which would allow a "back door" to be installed into the system. They determined that there was no way to ensure that the systems were bug-free, and did not contain malicious code.

The worst security errors found by the Hopkins study had been called to Diebold's attention five years earlier by Dr. Douglas W. Jones of the University of Iowa, a member of Iowa's Board of Examiners for voting systems. Dr. Jones says

that the Diebold story "represents a black eye" for the whole system of both state and Federal governments setting of voting equipment standards, because not only did the Diebold touch-screen system "pass all of the tests imposed by this standards process, but it passed them many times, and the source code auditors even gave it exceptionally high marks."

"Given this," Dr. Jones asks, "should we trust the security of any of the other direct recording electronic voting systems on the market?" He has called for de-certification of the Diebold equipment.

- The State of Maryland conducted a follow-up to the Hopkins-Rice study; in the follow-up, a group of computer experts found 328 software flaws, 26 of which they deemed critical. "If these vulnerabilities are exploited," they said, "significant impact could occur on the accuracy, integrity, and availability of election results."

Dangers of Internet Voting

Another just-released study recommends that the emerging trend toward Internet voting should be stopped in its tracks. Four computer-security specialists examined the new Defense Department program for Internet voting, known as SERVE (Secure Electronic Registration and Voting Experiment). SERVE is now just a prototype, which is intended to be used in some primaries, including the Feb. 3 South Carolina primary, and in a number of states in the November general elections. The SERVE system was created by the consulting firm Accenture, a renamed successor to the Arthur Anderson accounting firm, of Enron notoriety.

The authors note at the outset that all of the criticisms which have been made of DRE voting systems "apply directly to SERVE as well." But beyond that, they report that "because SERVE is an Internet- and PC-based system, it has numerous other fundamental security problems that leave it vulnerable to a variety of well-known cyber attacks," which "could result in large-scale, selective voter disenfranchisement . . . vote buying and selling . . . and/or vote switching even to the extent of reversing the outcome of many elections at once, including the Presidential election."

The authors of the SERVE study conclude that its vulnerabilities cannot be fixed, and that the system should be abandoned. They warn of the implications for the emerging trend for Internet voting. They warn that the system might appear to work flawlessly in the 2004 elections, but "the fact that no successful attack is detected does not mean that none occurred. Many attacks, especially if cleverly hidden, would be extremely difficult to detect, even in cases where they change the outcome of a major election."

A "successful trial" of the SERVE system "is the top of a slippery slope toward even more vulnerable systems in the future," the experts state; and they give, as an example, that "the existence of SERVE has already been cited as justification for Internet voting in the Michigan Democratic caucuses."

The 14th and 15th Amendments to the U.S. Constitution guarantee to citizens the right to vote, and the right to equal protection of the law—which means the right not only to cast a ballot, but to have it counted fairly.

The Constitutional right to vote is enforced by the Voting Rights Act of 1965—which is still on the books, despite combined efforts by right-wing Republicans and the Democratic National Committee to wipe it out. One of the provisions of the Voting Rights Act, is for the appointment of Federal voting examiners who are entitled to observe whether votes "are being properly tabulated."

But, if votes are being counted by a computer "black box," how can anyone know if they are being counted fairly? As studies have noted, it is possible to hide malicious code so that it is undetectable.

For example, Dr. David Jefferson, an election security expert at Lawrence Livermore Laboratories, states: "Any security expert will tell you that it is very easy to write hidden logic that behaves properly when being tested and only does its dirty work when used in a real election."

Thus, without some form of a paper trail, such as the recording on paper of individual votes, it is impossible to verify the results of a computerized tabulation of votes.

One solution being proposed, with Dr. David Dill of Stanford University in the forefront, is what is called a "voter-verifiable audit trail."

Dr. Dill has drafted a statement, which over 100 other computer scientists have signed, which says in part: "Computerized voting equipment is inherently subject to programming error, equipment malfunction, and malicious tampering. It is therefore crucial that voting equipment provide a voter-verifiable audit trail, by which we mean a permanent record of each vote that can be checked for accuracy by the voter before the vote is submitted, and is difficult or impossible to alter after it has been checked."

Bills have been introduced into both the House and the Senate to require a voter-verifiable audit trail on every voting system; this is called the "Voter Confidence and Increased Accessibility Act of 2003." It was first introduced in the House by Rep. Rush Holt (D-N.J.) in May 2003; Sen. Bob Graham (D-Fla.) introduced it in the Senate in December. The bills call for a permanent paper record to be created of each vote, which the voter can inspect and verify at the time of casting his ballot. The paper records would be securely maintained and would be the official record to be used in a recount. Additionally, there can be no undisclosed software in a voting system, and the source code must be open and available for inspection.

EIR is conducting its own study of the problem, and is not prepared to fully endorse these measures at this time, but we note that this is at least a step in the right direction. Unless the voter can verify his vote at the time it is cast, and unless there is a permanent, individual record which is available to be utilized in a recount if necessary, there no longer exists the right to vote and to have the vote fairly counted, as is guaranteed by the United States Constitution.