LaRouche: For Fair Elections, Ban Computer Voting Now!

by Edward Spannaus

Computer voting must be totally banned for the upcoming November Presidential elections, Democratic candidate Lyndon H. LaRouche told a large audience at a campaign event in Los Angeles on February 26.

What is needed is not just a protest, LaRouche said in response to a questioner. "We have to have some action now, before the election." This will not come from the courts, he noted, reminding his listeners of what happened to the last Presidential election at the hands of Justice Antonin Scalia and the U.S. Supreme Court.

The capability is already in place, to have "a fraudulent majority vote on a large scale, in the next election in November," and therefore, it must be stopped, LaRouche pointed out. He added that he and his associates are taking a number of steps on this, including working with members of Congress and others, to repeal or overturn the 2002 Help America Vote Act (HAVA), as well as to completely ban computerized voting.

The idea, LaRouche said, is "to *eliminate* the use of computer-controlled voting devices—*absolutely!*" This is necessary because computerized voting machines, by their nature, cannot be audited, LaRouche said. "You have no protection against massive fraud. And computer-based voting is the simplest way to carry out fraud. Diebold machines, and similar kinds of machines, are *inherently* fraudulent. They're *designed* for fraud. They've been tested: Hackers can get into these machines, and change the vote! Change the total vote, in a machine, by going into the relevant computer."

Back to Paper Ballots

In further discussions, LaRouche noted that the speed and complexity of computers creates an inherently dangerous and fraud-prone situation, because only a handful of people (who are often not even election officials, but private contractors) know what is going on. Using high-speed computers, perpetrators can carry out fraud and then clean it up afterwards, before anyone knows what has even happened.

Therefore, LaRouche is calling for a return to a universal paper ballot, which is hand-counted. If that requires more people to count the votes than computers, all the better. The more people involved, the more impediments to carrying out vote fraud. And secondly, LaRouche says, each voter should get a copy of their vote; this is the best deterrence to vote fraud.

To those who would object that this would be a slow, inefficient system of counting votes, LaRouche responds that a slow, ponderous vote-counting system, where people can watch what is going on, is the best way to prevent vote fraud and election-rigging.

In addition to emergency action by Congress to repeal HAVA and to ban computer voting, LaRouche is also supporting actions being undertaken in various states to ban computer voting, and to return to paper ballots.

A few examples of such actions in the states follow:

- In many states, the Ballot Integrity Project is calling for only paper ballots to be used, with a public hand count of ballots, and results recorded in triplicate and then secured.
- Two Ohio state Senators, a Democrat and a Republican, are calling for a delay in the approval of contracts for electronic voting machines, until a bipartisan legislative panel can assess the security risks associated with the implementation of HAVA.
- In California, voters and others filed suit against the State of California and Diebold, seeking to bar the state from using electronic voting and vote-tabulating software, unless specified security modifications are made.
- Activists in Maryland and California have called for

voters to use paper absentee ballots instead of touch-screen machines.

HAVA was passed in 2002 under two sets of false premises, along with heavy lobbying by GOP-linked voting machine companies and defense contractors.

The first false premise: The use of "modern" touch-screen devices would avoid the type of chaos that occurred in the 2000 Florida elections, with the fiasco of recounting punch-cards with their famous "hanging chads." Today, most of those who have studied the problem, regard touch-screen voting as a much bigger problem than punch-cards, since there is *no* paper trail with touch-screen voting, and no ability whatsoever, to conduct a recount. Fraud can be conducted in such a manner as to be virtually undetectable.

The second fraudulent premise: Touch-screen machines would allow disabled persons, particularly the blind, to vote in privacy. Thus, by 2006, every polling place used in a Federal election is required to have at least one touch-screen device, or another device "equipped for individuals with disabilities."

But rather than having different kinds of machines in polling places, many jurisdictions have opted for total replacement of old equipment, with touch-screen machines.

Or, take the case of Washington, D.C. Although the touch-screen machines were installed for voters with disabilities, others were permitted and even encouraged to use them, so that about 15,000 of 42,000 voters used them in the Jan. 13 primary.

Some handicapped activists have now become major defenders of touch-screen voting, and are vocal opponents of the "voter verification" movement for requiring touch-screen devices to produce an auditable paper trail.

Not so surprisingly, some of these activists seem to be on the payroll of at least one of the major touch-screen manufacturers. This is the Diebold company, which is actually in a self-proclaimed "partnership" with the National Federation for the Blind (NFB). Diebold settled a lawsuit involving its ATM machines by launching a joint project for a voice-guidance ATM machine. In addition to a cash settlement with the NFBs, Diebold announced a five-year, $1 million grant to an arm of the NFB. Jim Dickson, the leading lobbyist on voting for disability-related organizers, is reportedly an adviser to Diebold.

'A Threat to Our Democracy'

Not only was HAVA passed under false pretenses, but—as we demonstrated in a recent issue (*EIR*, Feb. 27)—it has been implemented by the Bush-Cheney Administration in a manner which has systematically sabotaged the development of guidelines and security standards for electronic voting machines. The new Election Assistance Administration, whose creation was stalled by the Administration for almost a year, has just announced that it will pass out $2.3 billion to help the states buy new voting equipment.

But by this time, under HAVA, there was also supposed to have been the development of standards for voting equipment, including security standards. But, in addition to stalling the EAC, which was to oversee the development of such standards, the Administration has even cut the budget for the the National Institute of Standards and Technology (NIST), which was designated to play the leading role in developing standards for voting equipment. In early February, the NIST announced that it had ceased all its HAVA-related activities.

Although the problems with computerized voting had been known for years, a number of studies came out during 2003 which identified major security flaws in Deibold and other systems.

Perhaps the best known of these, was one conducted by computer scientists from Johns Hopkins and Rice Universities, and released in July 2003. They examined Diebold software code for touch-screen machines, and found "stunning flaws" in the system's security. The authors of the study deteminined that there is no way to ensure that the systems are bug free, or that they do not contain "malicious code." The State of Maryland then conducted a follow-up to the Hopkins-Rice study, in which a group of computer experts found 328 software flaws, 26 of which they deemed critical. "If these vulnerabilities are exploited," the study concluded, "significant impact could occur on the accuracy, integrity, and availability of election results." The Congressional Research Service issued a study last November, more cautious than others, which also found significant security vulnerabilities in touch-screen systems.

Supporting LaRouche's warnings cited above, the CRS study stated "the more complex a piece of software is, the more vulnerable it is to attack." It 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."

One of the authors of the Hopkins study, Dr. Avi Rubin, participated as an election judge in the Maryland March 2 primary, in part prompted by accusations from Diebold that he was an academic scientist who knew nothing about how elections actually worked. In a report he posted on his website at the end of the day, Dr. Rubin reported that while some risks seemed to be less than he had expected, there were also some security issues which were worse than he had anticipated. Rubin concluded: "I continue to believe that the Diebold voting machines represent a huge threat to our democracy. I fundamentally believe that we have thrown our trust in the outcome of our elections in the hands of a handful of companies . . . who are in a position to control the final outcomes of our elections. I also believe that the outcomes can be changed without any knowledge of the changes by election judges or anyone else."