US voting machines: Will 2004 elections be electronically rigged?

Alex Lefebvre
24 December 2003

Recent revelations about US voting machinery companies and their products raise serious questions about the integrity of the electoral process in the US, as well as in other countries. These companies, which have intimate ties to the US right wing, operate with no real outside supervision. According to information that has emerged, their products' safety designs are so poor that they offer many opportunities to rig elections, especially for well-connected insiders.

The crucial issue has been the transition from paper or mechanical balloting to electronic balloting. In many electronic balloting systems, voters' information is simply stored electronically (known as Direct Recording Election, or DRE), as opposed to printing out a paper ballot that the voter can then check to see if the ballot matches his intentions. However, voting systems corporations generally claim that the software code that records votes is proprietary, and therefore deny outside personnel access to the code. When candidates or organizations have sued for the right to access the code, judges have ruled in favor of the voting systems corporations. The companies have also threatened to void warranties for the machines if they are inspected.

Voters who cast their ballots using any of a number of electronic voting systems have no way to check that their votes have been properly recorded. A New York election commissioner, Douglas Kellner, said: "Using electronic voting machines to count ballots is akin to taking all the paper ballots and handing them over to a couple of computer tech people to count them in a secret room, and then tell us how it came out. This is not an acceptable way of conducting elections in a democracy."

The democratic qualifications of the pre-DRE voting in the US should not be overstated. There have been numerous cases of elections rigged via manipulation of other voting machinery systems, or by altogether different means. However, the scope of unverifiability and the centralized, secretive nature of the tallying process create the conditions for an unprecedented attack on the public's democratic right to have its vote counted.

The Florida state primary elections of 2002, in which Jim McBride defeated former attorney general Janet Reno for the Democratic gubernatorial nomination, provided an example of the type of electoral irregularities that can be expected with DRE voting. Vote tallies in several precincts of Miami-Dade and Broward counties aroused Reno's suspicion, and she asked Professor Rebecca Mercuri, an expert in computer sciences and voting machine technology, to investigate.

In an interview with *Salon*, Mercuri said: "She called me because they saw the number rolling out of the machines, and they figured something was screwy. You would have places where there were over 1,300 [voters who had been polled] and there would be like one vote for governor." When asked about the process, the voting machinery supplier, Election System and Software (ES&S), sent a technician to recover the lost votes. Mercuri commented: "Basically ES&S comes in and they've got some sort of tool they stick in some part of the machine and they pull some data out of it. How can you trust that?"

The voting machinery industry is dominated by a few large corporations—Election Systems & Software (ES&S), Diebold and Sequoia. ES&S machines count between 55 and 60 percent of votes cast in the US; Diebold and ES&S machines put together count about 80 percent of US votes.

ES&S, formerly American Information Systems, enjoys impeccable conservative credentials and links to the clerical-fascist right. Its 1993-1994 CEO and 1992-1995 chairman, Chuck Hagel, became a Republican senator from Nebraska in 1996 and won his re-election in 2002 in elections where votes were counted entirely on ES&S machines. Although Hagel sold his entire stake in American Information Systems before becoming a candidate, he kept a $5 million stake in its parent company, the McCarthy Group. Hagel failed to disclose this fact on congressional documents.

ES&S also enjoyed the financial support of far-right California billionaire Howard Ahmanson. He provided capital to brothers Bob and Todd Urosevich, the founders of ES&S precursor American Information Systems. Bob Urosevich now heads the election division of Diebold, and Todd Urosevich is a top executive at ES&S. Ahmanson also funded the Chalcedon Foundation, a leading institution of the Christian Reconstructionist movement, which advocates the establishment of Christian theocracy and Old Testament law in the US, including the death penalty for homosexuals.

Diebold is largely controlled by staunch Republicans. Besides Urosevich, Diebold's current CEO Walden O'Dell is a leading fundraiser for George Bush's re-election campaign; he recently declared he was "committed to helping Ohio deliver its electoral votes to the president next year." During the 2000 and 2002 election campaigns, Diebold donated over $200,000 exclusively to the Republican Party.

Sequoia is largely controlled by the British cash-printing firm De La Rue. Its management has a remarkable record of dishonesty: executives Phil Foster and Pasquale Ricci were convicted in 1999 of paying Louisiana commissioner of elections Jerry Fowler an $8 million bribe to buy their voting machines. These convictions took place in the context of a massive election scandal in Louisiana involving connections with organized crime, in which Sequoia executives gave immunized testimony against state officials. Ricci in particular was suspected of having mob links.

Sequoia is also linked to the Bush family: De La Rue's corporate parent, private equity firm Madison Dearborn, is a partner of the Carlyle Group, the investment firm that employs the current president's father, former president George Herbert Walker Bush.

After the theft of the 2000 election, the Bush administration tried to blunt opposition to its undemocratic installation by passing a voting reform act. The bill, titled Help America Vote Act (HAVA), finally passed in October 2002, shortly before the 2002 election cycle. It rallied the support of several liberal political organizations, notably Public Citizen and the League of Women Voters.

The legislation requires that electronic voting systems be in place for the

next presidential election of 2004. It includes $4 billion in funding for states to replace voting equipment—funds that would go straight from Congress and the Bush administration to their backers in the voting machinery industry. The bill did not directly indicate which voting machinery should be adopted. However, the amount of funding it provided per precinct—$3,200—was enough to fund DRE machines (which cost $3,000-$4,500), but not optical scanners, the main competitors of DREs. Optical scanners, in which voters fill out bubble sheets, cost $4,500-$6,000 apiece and are less accessible to the handicapped.

Moreover, although HAVA specified that voting machinery should meet certain standards, these standards have not yet been published due to the failure of the Republican-controlled Congress to appoint a commission. The standards may not be in place until 2006, at which point states will already be under obligation to have purchased new equipment. Other legal loopholes exploited by the voting machine companies include selling machines that have the capacity to print out paper ballots after the election is finished as machines that "create a paper trail." However, as these machines often do not print out ballots that the voter himself inspects, this distinction is specious.

States are still in the process of attempting to reach HAVA compliance, and information on what systems will be in use during the elections is spotty. However, 36 states have accepted HAVA funds and plan to replace substantial portions of their voting equipment. Three states (Alabama, Alaska, and Maryland) have not applied for HAVA funding, but Maryland is considering updating its equipment to all-Diebold DRE voting with no paper trail features. Eleven states—Arkansas, Florida, Illinois, Indiana, Maine, New Hampshire, South Carolina, Utah, Vermont, Virginia and West Virginia—have not yet decided whether to apply for HAVA funds.

A bitter controversy has emerged over the reliability and security of DRE voting. DRE voting systems have many proponents: voting systems corporations and their backers, handicapped organizations that view DRE voting as more accessible, and liberal groups claiming concern for possible disenfranchisement of poorer voters as a result of using antiquated machinery. However, work by a large number of people—investigative journalists, computer security professionals and students, and voting industry workers—has shown that current DRE voting systems have massive and critical security flaws.

Not least among these are the risk of computer fraud by the voting industry itself. Although counties require companies' software and machinery to pass tests, there is no way to prove that the company uses that same software on election day. In fact, Diebold has already been caught secretly switching code after its machines had been tested in Alameda County, California, according to a November 6 story in the *Oakland Tribune*. Diebold workers also reported that the company switched software in Georgia between tests and the 2002 elections.

These concerns are compounded by the fact that most DRE systems—including all ES&S machines—have internal modems connecting them to external computers. Hackers able to decipher voting machinery code or voting industry programmers could thus issue instructions to the voting machines during or after the elections, after testing of the machines had taken place.

David Dill, a computer science professor at Stanford University, commented: "The ability to install patches or new software that wasn't certified has many risks, including the introduction of new bugs and more opportunities for tampering. It is even more risky if different patches can be installed at the last minute in particular jurisdictions. This opens the possibility of customized tampering by people who know exactly which races they want to affect, or bugs that are even less likely to be caught because they occur only in a small number of locations. Of course, even if the certified code is frozen, it is easy to think of ways that undetectable back-doors [for tampering] could be installed in the software so that someone at the election site could choose the winner of the election."

Perhaps the most damning revelation came in January 2003: voting activists discovered that much of Diebold's code for its election machinery had been available for an unspecified amount of time on a public, insecure ftp server. Anyone who knew about the server could thus download and examine the code, or even modify it and send it back to the Diebold server. According to blackboxvoting.com, the available files included hardware and software specifications, the central vote-counting program, and "replacement files" for Diebold and Windows software supporting the vote-counting program. Blackboxvoting.com later revealed that Sequoia files were also available on a public ftp server.

Some of the available Diebold files were particularly damaging from the point of view of computer security: they included diagrams of communications links, passwords, encryption keys, testing protocols and simulators.

Computer scientists at Johns Hopkins and Rice universities published an analysis of sections of the publicly available Diebold code. It is available at http://avirubin.com/vote.pdf. The report found many substantial flaws in Diebold's DRE technology. Firstly, voters validate their identity by presenting a "smart card" electronic identity card that turns itself off once the voter has voted. However, the report found that it would be simple and inexpensive to buy a similar card and program it to allow a voter to vote as many times as he wanted. Poll workers would have similar opportunities to directly and unverifiably tamper with vote totals.

The report also found that the transmission systems between voting machines and central computers were non-encrypted, allowing for easy modifications of vote totals by hackers while such messages are in transit. It noted that the use in the election programming of C++, a programming language known for its relative vulnerability to hacking, indicated the company's unserious approach to computer security.

Perhaps most importantly, the report found "no evidence of any change-control process that might restrict a developer's ability to insert arbitrary patches to the code. Absent such processes, a malevolent developer could easily make changes to the code that would create vulnerabilities to be later exploited on Election Day."

Diebold's response to the charges was to claim that one of the report's authors, Avi Rubin, had a conflict of interest, as he held stock in a smaller, rival voting-machinery company, and to threaten lawsuits against web sites posting its code for evaluation. The state of Maryland, which is preparing to equip itself solely with Diebold electoral machinery, hired SAIC, a defense contractor with CIA ties, to evaluate the security of its software. SAIC's heavily redacted public report agreed with most of the Johns Hopkins/Rice report's technical findings, but speciously argued that its understanding of Diebold's source code was flawed and that the state of Maryland's "voting environment" would prevent any vote-tampering.

Key questions, to which there are still no definite answers, include: Was this remarkable breach of security a complete oversight, or were there elements inside Diebold who deliberately allowed the files to be placed where outside operatives could find them? Who accessed the Diebold files? What, if any, changes were made? More generally: Do right-wing political operatives in the US now have the ability to electronically fix elections by tampering with voting software?