The Nation.

ARTICLE | *posted July 29, 2004 (August 16, 2004 issue)*

How They Could Steal the Election This Time

RONNIE DUGGER

On November 2 millions of Americans will cast their votes for President in computerized voting systems that can be rigged by corporate or local-election insiders. Some 98 million citizens, five out of every six of the roughly 115 million who will go to the polls, will consign their votes into computers that unidentified computer programmers, working in the main for four private corporations and the officials of 10,500 election jurisdictions, could program to invisibly falsify the outcomes.

The result could be the failure of an American presidential election and its collapse into suspicions, accusations and a civic fury that will make Florida 2000 seem like a family spat in the kitchen. Robert Reich, Bill Clinton's Labor Secretary, has written, "Automated voting machines will be easily rigged, with no paper trails to document abuses." Senator John Kerry told Florida Democrats last March, "I don't think we ought to have any vote cast in America that cannot be traced and properly recounted." Pointing out in a recent speech at the NAACP convention that "a million African-Americans were disenfranchised in the last election," Kerry says his campaign is readying 2,000 lawyers to "challenge any place in America where you cannot trace the vote and count the votes" [see Greg Palast, "Vanishing Votes," May 17].

The potential for fraud and error is daunting. About 61 million of the votes in November, more than half the total, will be counted in the computers of one company, the privately

PRINT THIS ARTICLE

EMAIL THIS ARTICLE

WRITE TO THE EDITORS

TAKE ACTION NOW

SUBSCRIBE TO THE NATION

Click here to help prevent disenfranchisment in this year's election.

Ronnie Dugger wrote the definitive warning essay about the dangers of computerized vote-counting in *The New Yorker* of November 7, 1988. Research support was provided by The Nation Institute. Dugger wishes to acknowledge the special assistance of Frances Mendenhall, Pokey Anderson, Peter Neumann, Rebecca Mercuri, Roxanne Jekot and David Jefferson, and his debt to hundreds of other reporters whose work cannot be properly credited here.

held Election Systems and Software (ES&S) of Omaha, Nebraska. Altogether, nearly 100 million votes will be counted in computers provided and programmed by ES&S and three other private corporations: British-owned Sequoia Voting Systems of Oakland, California, whose touch-screen voting equipment was rejected as insecure against fraud by New York City in the 1990s; the Republican-identified company Diebold Election Systems of McKinney, Texas, whose machines malfunctioned this year in a California election; and Hart InterCivic of Austin, one of whose principal investors is Tom Hicks, who helped make George W. Bush a millionaire.

CONTINUED

About a third of the votes, 36 million, will be tabulated completely inside the new paperless, direct-recording-electronic (DRE) voting systems, on which you vote directly on a touch-screen. Unlike receipted transactions at the neighborhood ATM, however, you get no paper record of your vote. Since, as a government expert says, "the ballot is embedded in the voting equipment," there is no voter-marked paper ballot to be counted or recounted. Voting on the DRE, you never know, despite what the touch-screen says, whether the computer is counting your vote as you think you are casting it or, either by error or fraud, it is giving it to another candidate. No one can tell what a computer does inside itself by looking at it; an election official "can't watch the bits inside," says Dr. Peter Neumann, the principal scientist at the Computer Science Laboratory of SRI International and a world authority on computer-based risks.

The four major election corporations count votes with voting-system source codes. These are kept strictly secret by contract with the local jurisdictions and states using the machines. That secrecy makes it next to impossible for a candidate to examine the source code used to tabulate his or her own contest. In computer jargon a "trapdoor" is an

opening in the code through which the program can be corrupted. David Stutsman, an Indiana lawyer whose suits in the 1980s exposed a trapdoor that was being used by the nation's largest election company at that time, puts it well: "The secrecy of the ballot has been turned into the secrecy of the vote count."

  According to Dr. David Dill, professor of computer science at Stanford, all elections conducted on DREs "are open to question." Challenging those who belittle the danger of fraud, Dill says that with trillions of dollars at stake in the battle for control of Congress and the presidency, potential attackers who might seek to fix elections include "hackers, candidates, zealots, foreign governments and criminal organizations," and "local officials can't stop it."

Last fall during a public talk on "The Voting Machine War" for advanced computer-science students at Stanford, Dill asked, "Why am I always being asked to prove these systems aren't secure? The burden of proof ought to be on the vendor. You ask about the hardware. 'Secret.' The software? 'Secret.' What's the cryptography? 'Can't tell you because that'll compromise the secrecy of the machines.'... Federal testing procedures? 'Secret'! Results of the tests? 'Secret'! Basically we are required to have blind faith."

CONTINUED ▶

Get The Nation at home (and online!) for 75 cents a week!

If you like this article, consider making a donation to The Nation.

PRINT THIS ARTICLE | EMAIL THIS ARTICLE | WRITE TO THE EDITORS | TAKE ACTION NOW

MOBILE | ABOUT US | CONTACT | MEDIA KIT | PRIVACY POLICY | + MY YAHOO!

Copyright © 2006 The Nation