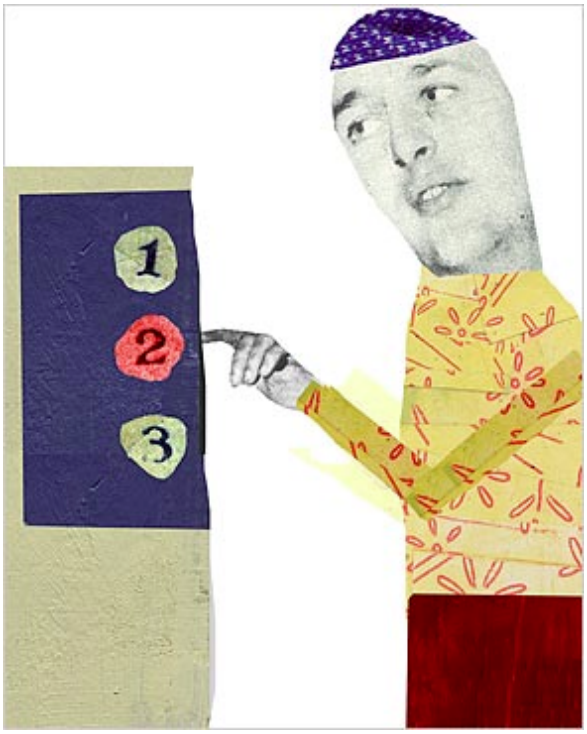
To print this page, select "Print" from the File menu of your browser



Hacking democracy?

Computerized vote-counting machines are sweeping the country. But they can be hacked -- and right now there's no way to be sure they haven't been.

By Farhad Manjoo

PRINT EMAIL

Feb. 20, 2003 | During the past five months, Bev Harris has e-mailed to news organizations a series of reports that detail alarming problems in the high-tech voting machinery currently sweeping its way through American democracy. But almost no one is paying attention.

Harris is a literary publicist and writer whose investigations into the secret world of voting equipment firms have led some to call her the Erin Brockovich of elections. Harris has discovered, for example, that Diebold, the company that supplied touch-screen voting machines to Georgia during the 2002 election, made its system's sensitive software files available on a public Internet site. She has reported on the certification process for machines coming onto the market -- revealing that the software code running the equipment is seldom thoroughly reviewed and can often be changed with mysteriously installed "patches" just prior to an election. And in perhaps her most eyebrow-raising coup, she found that Sen. Chuck Hagel, a Nebraska Republican, used to run the company that built most of the machines that count votes in his state -- and that he still owns a stake in the firm.

Harris hasn't been alone in making such discoveries. A small group of writers, technologists and activists is working hard to convince elections officials all over the country that their rush to upgrade aging punch-card machines with seemingly more reliable touch-screen systems is dangerous. But so far neither the general public nor elections officials appear too worried.

It's not hard to see why: If you look at some of the conspiracy theory rhetoric on the Web spawned by the work of Harris and others, it becomes all too easy to dismiss the whole campaign as sour grapes. There is no smoking-gun evidence to support the conclusion that Hagel's landslide Senate victory in 2002 benefited from voter fraud. The same is true for several unexpected Republican victories in Georgia last year -- during which the entire state used touch-screen machines for the first time.

But Harris herself is no conspiracy nut. Her facts check out. Nor is she an ideologue. Her stories on voting machines are based not on her politics but on serious, in-depth investigative reporting. Since October, she's spoken to dozens of people in the voting world, from elections officials to "systems certifiers" to engineers whom she calls whistle-blowers. She's detailed some of her findings on her Web site, but she says they aren't the whole story -- which she'll tell in a book, "Black Box Voting," to be published in May.

The facts Harris and others lay out ought to give many election officials pause. Touch-screen voting machines aren't especially reliable; there are documented cases in which they have frozen, broken down and tabulated incorrectly during actual, binding elections. They're also not immune to hacks. Though voting companies will confidently tell you about their myriad security policies, the fact is that these machines run software, and software can be tampered with: An election result *could* be changed without anyone being the wiser. And perhaps worst of all, the machines and the companies that make them are shrouded in secrecy. What really happens in a touch-screen machine when you select your candidate? In most cases, everything probably goes as it should -- but there is no way to know for sure.

Indeed, the conspiracy theories, regardless of their validity, nevertheless highlight the main problem with electronic machines. Because they leave no paper trail -- the vote count is registered only electronically in the machine -- the results that the new machines deliver are open to dispute by people who have cause to be suspicious. For instance, Charlie Matulka, Hagel's Democratic opponent in Nebraska last year, believes that he might have won the race -- though the official count put him at about 15 percent of the vote.

Bev Harris doesn't believe that anything went wrong in Nebraska, but that's not the point. She wonders how you can prove that everything went well when what goes on inside a voting machine isn't accessible by the public.

The same problems are in play with respect to the Georgia elections. "I don't think that there was anything wrong, but I can't show that there wasn't," says David Dill, a computer scientist at Stanford University. Dill is trying to get Santa Clara County, the home of California's Silicon Valley, to reject electronic machines that don't produce a paper trail. "And it always frustrates me when I read a conspiracy theory and I can't find some way to dismiss it -- it bothers me that I can't show people that they're full of it."

Harris first became interested in elections last fall, when she read an article that detailed some problems with electronic voting systems -- specifically that the machines store their data in a way that isn't readily "auditable" and that they are made by companies that tend to be secretive about their processes and investors.

"Something just clicked," Harris says of reading that article, "and in this climate of a year of corporate shenanigans, I said, 'I'll just do a quick search to see who controls some of these companies.'"

Harris, who runs a P.R. firm in Seattle that does work for "unknown authors that need some publicity," had always hankered to do investigative journalism. She once publicized a book for Jack Anderson, the Pulitzer Prize-winning Washington Post reporter, and his stories of investigative reporting had intrigued her.

She began by looking into Election Systems & Software, the world's largest election supply company, based in Omaha, Neb. Harris quickly found that ES&S was owned, in part, by a merchant banking holding company called the McCarthy Group and that the firm's chairman, Michael McCarthy, was Chuck Hagel's campaign treasurer. After searching news archives, Harris found that during Hagel's first campaign, in 1996, the Nebraska media reported that he had been president of ES&S -- which at the time was called American Information Systems -- between 1992 and 1995. But the articles suggested that Hagel was no longer affiliated with the voting equipment company. Harris saw election records that showed Hagel still holding between $1 million and $5 million worth of stock in McCarthy, which owned about 25 percent of ES&S.

Harris had stumbled on what seemed to be a striking conflict of interest -- a U.S. senator owned a share in a company that built all the vote-counting machines in his state. She put up the relevant documents on her site, "and immediately I knew I'd hit a sore spot," she says, "because right away I got a threat letter from ES&S."

The letter from ES&S's attorneys demanded that Harris take down her article. "While you claim that your article is all based upon verifiable facts, even if true, which ES&S disputes, you should be aware that such 'facts,' or the implications therefrom, when presented in a false fashion, constitute defamation or defamation by implication as well as the privacy tort of false light," the attorneys said.

It's not clear what ES&S meant to convey by such a letter, but Harris didn't take down her article. "What I would certainly do if they launched a lawsuit is, we'd have a field day with discovery," she jokes now. ES&S did not return Salon's phone calls for comment.

Harris thought it odd that McCarthy's underlying assets, including the voting company, were not disclosed in Hagel's election filings, and she tipped off the Hill, a newspaper that covers Congress. Late in January, the paper reported that Hagel's omission might have constituted a Senate ethics "disclosure issue."

Did Nebraskans know of Hagel's affiliation with the voting company? Lou Ann Linehan, Hagel's chief of staff, says that the senator has been upfront with all of his business dealings. Although he owns a share in McCarthy, and McCarthy owns a share in ES&S, Linehan says there is "absolutely no affiliation" between the senator and the voting company. Hagel's indirect ownership of ES&S is tiny, his staff points out -- he owns "less than 2 percent" of McCarthy, and McCarthy owns only about a quarter of ES&S. Linehan denied there was any ethical problem with the way Hagel disclosed his McCarthy holdings. Members of Hagel's staff pointed to a letter to the Hill by William Canfield, a Senate ethics expert, that said that "Sen. Hagel has fully met his obligation, under the statute and the committee's guidance, in publicly disclosing this particular investment."

Linehan said there's nothing irregular about a person who used to run a voting-machine firm running for office. "Maybe if you're not from Nebraska and you're not familiar with the whole situation" you would have questions, she says. "But does it look

questionable if there's a senator who is a farmer and now he votes on ag issues? Everybody comes from somewhere."

Nebraska was considered a "safe state" for Republicans in 2002. Most political commentators believed Hagel's opponents -- Phil Chase, an independent, John Graziano, a Libertarian, and Charlie Matulka, the Democratic candidate -- did not stand a chance. And according to the official count, Hagel trounced the opposition. He won about 400,000 votes -- Matulka, in second place, won just over 70,000.

Matulka believes that Hagel's landslide doesn't indicate a victory but something underhanded with the vote. "Why in the world would anybody with the election company want to run for office? It's like the fox in the henhouse -- they said they didn't do it, but they got feathers in the mouth." Matulka can't show any feathers, however: There appears to be not a shred of evidence to suggest that Hagel didn't honestly win his landslide, and the only thing Matulka has going for him is his hunch.

Then again, there's nothing to *disprove* what Matulka says, either. And that's the problem.

Many of the counties in Nebraska in 2002 used optical-scan ballots, in which votes cast on a paper ballot are counted in a machine; but several big counties, constituting a large part of the Nebraska electorate, used touch-screen machines. Matulka says that the lack of paper ballots that can be counted manually makes him suspicious. "What's so wrong with manually counting the votes?" he asks. "They've done away with the damn paper trail."

Linehan sees nothing wrong with the way the vote was conducted. "Nebraska is a very special place," she says, "and when you go to vote in Nebraska, the people at the polls know who you are. Sen. Hagel won by 83 percent of the vote, and there's no doubt he won by an overwhelming majority. And you get poll workers there who would -- if something was wrong, people would know what's going on."

According to elections firms and election officials, the software and hardware in voting machines is thoroughly inspected and tested before the systems are certified and put on the market for sale to county election directors. Doug Lewis, who heads the Election Center -- a nonprofit management division of the National Association of State Election Directors, which handles part of the voting-machine certification process -- said that "the likelihood of doing something to [a machine] without detection is very, very small."

Lewis says that if you have "malicious code in the system" -- such as a simplistic virus, perhaps, designed to change a vote cast for one candidate into one for his opponent -- the code will be caught in the testing phase of the certification process: "It will not compile right. The testing itself would discover this." Moreover, Lewis says, the testing labs simulate actual voting on each type of machine. The test, which is 163 hours long, "puts tens of thousands of votes into the system, and we know what the outcome is supposed to be."

Lewis says that no voting system ever designed has been perfect. If it's "created by man, it can be destroyed by man," he says. But he believes that several rounds of testing make the machines about as good as we can get them.

Harris finds that hard to believe. In the course of her research, she's uncovered what she says is evidence to suggest that the testing phase of the certification process is flawed. One person she holds up as an example is Dan Spillane, an engineer who worked on the software at a company that made electronic voting machines. Spillane says that national testing labs "are very much like Arthur Andersen in the Enron case": They don't do a very good job. The company Spillane worked for -- he prefers not to have the name published -- would pass systems "with problems that we knew about internally, problems with severity level 1, the highest" on to the testing labs, and the labs would certify the equipment. (Spillane was fired from the company, and he says he plans to sue the firm for wrongful termination.)

Lewis' claim that malicious software "won't compile" is also suspect. Malicious software abounds on computers; on every platform, in every application, from Microsoft Word to e-mail, are bad bits of code. There's no technical reason why one renegade coder at a voting company couldn't slip some pro-Republican or pro-Democratic code into his firm's systems. Computer scientists fear that malicious code can be written so as to evade detection during the testing process, going live only on Election Day.

And for each security procedure that a company might put in place to defeat such efforts, hackers will come up with more sophisticated methods to get around them, says Stanford's David Dill. Recently, worried about the possibility that paperless electronic voting machines will become the national standard, Dill decided to see what others in his field -- people who know about computers and the limits of their security -- could do to let election officials know of the danger.

"Almost any computer scientist I would walk up to would agree with me," says Dill. So he put up a statement of his beliefs regarding electronic voting, and he invited other computer scientists to sign on to it. The statement reads:

"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. Many of the electronic voting machines being purchased do not satisfy this requirement. Voting machines should not be purchased or used unless they provide a voter-verifiable audit trail; when such machines are already in use, they should be replaced or modified to provide a voter-verifiable audit trail. Providing a voter-verifiable audit trail should be one of the essential requirements for certification of new voting systems."

The response to Dill's petition was remarkable. In a few weeks, he'd garnered more than 100 signatories, including some of the biggest names in computer security.

Dill recently learned that Santa Clara County is considering purchasing electronic machines that don't print out an audit trail, and he's become an outspoken local advocate against them. He says he's somewhat surprised that election officials haven't taken his and other technologists' concerns more seriously. "I must admit to a certain amount of frustration showing up at these county meetings and hearing that everyone's getting their information from the vendor," he says. "And basically I think that once you get out into the real world, nobody knows who these computer scientists are."

Still, Dill says, his group does "seem to be changing the equation" in Santa Clara, and he thinks that if the county goes the way he'd like -- forcing voting firms to put an audit trail into the machine --- other parts of the country may be more inclined to follow.

Harris has also been popularizing Dill's cause, because she fears that if paperless electronic machines aren't stopped, dire consequences will follow. I asked Harris if she wonders whether she could be too late -- whether there's already been an election in which an electronic machine has produced the wrong result.

"I have worries about Georgia," Harris said. In 2002, the entire state of Georgia used touch-screen machines provided by Diebold. Harris has found an FTP site run by Diebold that allowed anyone with access to the Internet to peruse what might have been important software files concerning the machines used in the state. It's unclear what files were on that site, but Harris wonders whether the programs, which could have been tampered with, were actually loaded onto the voting machines. More recently, Harris found that in an effort to fix a problem that was causing 5 percent of the machines in Georgia to freeze up, Diebold administered a software "patch" to all 22,000 machines in the state shortly before the November election. The patch -- which changes the code on the machine -- was certified "by phone," according to a Georgia election official quoted by Harris.

Joseph Richardson, a spokesman for Diebold, denied that a patch had been applied to the Georgia machines: "We have analyzed that situation and have no indication of that happening at all." In regard to the FTP site, he said, "Our review of this matter indicates there is no merit to the insinuations of security breaches in the Diebold Election Systems solutions. The old Global Election Systems site has been taken down because it contained old, out-of-date material. For 144 years, Diebold has been synonymous with security, and we take security very seriously in all of our products and services." (Georgia elections officials did not respond to phone calls for comment.)

Republicans enjoyed great success in Georgia last year. Defying pre-race polls, voters chose Sonny Perdue, the state's first Republican governor in 135 years, and, for the Senate, the Republican Saxby Chambliss over the incumbent Democrat Max Cleland. After the race, many pundits wondered what had caused the GOP sweep: Was it the president's nonstop campaigning? Had the Democrats dropped the ball on homeland security?

There's every reason to believe that an explanation can be found among those conventional theories. The problem with the widespread use of electronic voting machines, though, is that there's nothing to stop people from thinking that something else, something altogether baser than pure politics, got in the way.

- - - - - - - - - - - -

About the writer
Farhad Manjoo is a staff writer for Salon Technology & Business.

Sound Off
Send us a Letter to the Editor

Related stories
Voting into the void
New touch-screen voting machines may look spiffy, but some experts say they can't be trusted.
By Farhad Manjoo
11/05/02

Guns, lies and the Internet in South Carolina
Field & Stream's Web site was associated with a voter's guide accusing a Democratic Senate candidate of being anti-gun. One problem: He's a member of the NRA.
By Farhad Manjoo
11/01/02

Political spam: Get used to it
An outraged constituent is suing Elizabeth Dole's campaign for sending junk e-mail. Is spam from politicians a crime -- or a vital First Amendment right?
By Katharine Mieszkowski
11/20/02

GO TO: Salon.com >> Technology

Salon, 22 4th Street, 16th Floor, San Francisco, CA 94103
Telephone 415 645-9200 | Fax 415 645-9204
E-mail | Salon.com Privacy Policy | Terms of Service