Automating elections: electronic voting machines have made mistakes too

by Roberto Verzola

The most common reason for abandoning manual elections in favor of automated ones is to eliminate the clerical errors that have been part and parcel of manual election counts. The frequent occurrence of such clerical errors, which election officials may ignore if the correction will not materially change the outcome, can hide more substantial alterations purposely intended to change the outcome of an election.

In the popular consciousness, however, computers have acquired such an image of precision and accuracy, if not infallibility, that the public, the media and policy makers almost take it for granted that automated elections and electronic voting will eliminate the errors so typical of manual election processes, not to mention delivering the results “within hours”.

This paper reviews the errors and other problems that have actually occurred in automated election systems in various countries. Some problems have been serious enough that countries like the Netherlands have actually abandoned electronic voting machines and gone back to paper and pencil.¹ Other problems have been cropping up with surprising regularity, especially in the U.S., where nearly 90% of counties were already automated in 2007, up from around 87% in 2006. The study of these problems can lead to a deeper appreciation of the strengths and weaknesses of automated machines as applied to a democratic process like an election.

One of the biggest databases of election-related problems in an automated context is the Election Incident Reporting System (EIRS) project of the Verified Voting Foundation in the U.S.² The EIRS database contains reports of more than 42,000 election “incidents” which occurred in the U.S. in 2004-2005, with a detailed description of each incident. The database provides a detailed peek into the nature of problems associated with automated elections. To get a sense of the EIRS reports, download the file http://verifiedvotingfoundation.org/downloads/resources/documents/ElectronicsInRecentElections.pdf.

The EIRS incidents are classified into 19 major categories. The categories and the frequency of each incident (also expressed as a percentage of the total) are listed in Table 1. (Many incidents belong

to more than one category, in which case, the first category listed was used for the classification.)

The top five problems, accounting for 77.3% of the total, were: registration-related problems (36%), polling place inquiries (17.3%), absentee ballot-related (9.6%), others (9.1%), and machine problems (5.4%).

Table 1: Election-related problems in an automated context

<table>
<thead>
<tr>
<th>Election problem reported</th>
<th>Count</th>
<th>% of total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration-related</td>
<td>15,404</td>
<td>36.0%</td>
</tr>
<tr>
<td>Polling place inquiry</td>
<td>7,404</td>
<td>17.3%</td>
</tr>
<tr>
<td>Absentee ballot related</td>
<td>4,122</td>
<td>9.6%</td>
</tr>
<tr>
<td>Others</td>
<td>3,896</td>
<td>9.1%</td>
</tr>
<tr>
<td>Machine problem</td>
<td>2,293</td>
<td>5.4%</td>
</tr>
<tr>
<td>Other polling place problem</td>
<td>2,248</td>
<td>5.2%</td>
</tr>
<tr>
<td>Voter intimidation</td>
<td>1,763</td>
<td>4.1%</td>
</tr>
<tr>
<td>Provisional ballot</td>
<td>1,181</td>
<td>2.8%</td>
</tr>
<tr>
<td>Identification related</td>
<td>1,075</td>
<td>2.5%</td>
</tr>
<tr>
<td>Long lines</td>
<td>1,072</td>
<td>2.5%</td>
</tr>
<tr>
<td>Other ballot-related</td>
<td>794</td>
<td>1.9%</td>
</tr>
<tr>
<td>Disability access</td>
<td>539</td>
<td>1.3%</td>
</tr>
<tr>
<td>Criminal status related</td>
<td>354</td>
<td>0.8%</td>
</tr>
<tr>
<td>Late opening</td>
<td>208</td>
<td>0.5%</td>
</tr>
<tr>
<td>Insufficient number of ballots</td>
<td>129</td>
<td>0.3%</td>
</tr>
<tr>
<td>Early closing</td>
<td>121</td>
<td>0.3%</td>
</tr>
<tr>
<td>Non-English language assistance</td>
<td>111</td>
<td>0.3%</td>
</tr>
<tr>
<td>Student status</td>
<td>74</td>
<td>0.2%</td>
</tr>
<tr>
<td>Unable to read ballot</td>
<td>51</td>
<td>0.1%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>42,839</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

Manipulating turnout

The first two problems, “registration related” and “polling place inquiry”, together with problems such as “other polling place problems”, “voter intimidation”, “identification related”, “long lines”, “criminal status related”, “late opening”, “insufficient number of ballots”, and “early closing” all affect voter turnout. Polling places with these problems are bound to see a low turnout, while those which are relatively free from these problems are bound to see a better turnout.

So, here is a simple way by which election results, automated or not, can be manipulated by
simply making sure through various means, fair or foul, of a high turnout in one’s bailiwicks and a low turnout in the opponent’s bailiwicks.

This election tactic is the focus of the 2002 film “Unprecedented: The 2000 Presidential Election” by U.S. journalist Greg Pallast. The film shows how 54,000 (the estimate now runs to 91,000) black voters, mostly Democratic, were illegally removed from the voters’ list of Florida just before the 2000 U.S. presidential elections.³,⁴ George Bush went on to win in Florida by a mere 537 votes,⁵ which eventually gave him the U.S. presidency.

Even “machine problems” can affect turnout. When machines stop working, screens refuse to respond properly, printers jam, etc., the pace of voting slows down considerably, long lines start forming, and many people will be unable to vote.

**Machine problems galore**

Aside from their impact on turnout, the following types of machine problems have been documented:

*Uninitialized machines.* Voters and poll officials in a Pennsylvania county were unable to confirm that counts inside 120 voting machines were initialized to zero, because the machines refused to issue “zero-count” printouts when the polling places opened.⁶ Uninitialized machines are the electronic equivalent of ballot boxes which have been stuffed with ballots even before the voting has started.

*Votes/choices not counted or lost.* Here is one account from the U.S.: “A North Carolina early voting test in the 2002 general election of six touch-screen machines made by [ES&S] uncovered a software problem that led to 436 uncounted votes. Local officials were further frustrated when a company representative acknowledged that they had seen the glitch before in a nearby county – and hadn’t shared the information.”⁷ A 2002 runoff in Wellington, Florida, was won by five votes. Although

---


⁴ See the video’s website at http://www.unprecedented.org/votermarch.htm.


it was the only contest on the ballot, 78 ballots did not register any vote. When Virginia voters in a U.S. election in November 2003 saw an “X” appear, and then disappear, beside one candidate’s name on some voting machines, they asked that the machines be tested. Officials found that the machines had deleted about 1% of the votes cast for a particular candidate. The candidate, Rita Thompson, eventually lost the race. On March 2, 2004, in San Diego County in California, polling place inspector John Pilch reported: “We lost 10 votes, and the Diebold technician who was there had no explanation.” These problems are dwarfed by the 2000 fiasco, when, as a Science article described it, “more than 1.3 million votes were lost because of ballot design problems.”

Candidates/choices reversed. At a primary election in Florida in 2002, an undetermined number of votes cast for the Democratic candidate for governor were assigned instead to Republican candidate for governor Jeb Bush, supposedly by a “misaligned” touch-screen.

Contests not counted. According to an ACM article, “in 2000, a Sequoia DRE machine was taken out of service in an election in Middlesex County, NJ, after 65 votes had been cast. When the results were checked after the election, it was discovered that none of the 65 votes were recorded for the Democrat and Republican candidates for one office, even though 27 votes each were recorded for their running mates.”

Ballots not counted. In a 2003 election in New Mexico, U.S., involving 48,000 electronic ballots, 12,000 ballots were ignored by the voting machines. Officials noticed the “software glitch” only after ten days. In another election the same year in Florida, U.S., for the state Senate, 137 blank electronic ballots were cast in a race with a winning margin of 12 out of 10,844 votes cast. With such a small margin, a recount should have been conducted, according to state law. However, since no paper ballot or audit trail existed, no recount was possible. Another report from Phillips County in Arizona, U.S., in 2006: “432 of 2,011 [Democratic] ballots had ’mistakenly been counted as Republican ballots, effectively nullifying them’.”

Wrong winner comes out. From a 2002 report in Johnson County in Kansas: “Results were

---

10 Verified Voting Foundation, see above.
12 Leopold, see above.
13 Dill et al., see above.
14 Gaither, see above.
15 Gaither, see above.
16 Theisen, see above.
misreported in six races. The system miscounted hundreds of votes, and a recount was ordered.”\textsuperscript{17} And a 2006 report in Pottawamie County in Indiana: “A machine count of the absentee ballots showed Sciortino 79, Duran 99; but a subsequent hand count have the correct count: Sciortino 153, Duran 25.”\textsuperscript{18}

\textit{Voting more than once.} According to a report by the Verified Voting Foundation on March 2, 2004, “at least one voter was able to vote twice on her ‘smart card’, and 10 votes were inexplicably lost.”\textsuperscript{19}

\textit{Votes exceed the total number of registered voters.} In the 2003 elections in Boone County in Indiana, U.S., whose registered voters did not exceed 19,000, electronic voting machines recorded 144,000 votes.\textsuperscript{20}

\textit{Negative votes.} Electronic voting machines have even recorded negative votes for candidates. During the 2000 U.S. presidential election counting in Volusia County in Florida, from a single precinct with 585 registered voters of which 412 actually voted, Gore got a negative 16,022 votes, while Bush picked up 2,813. The correct results after a manual count: Bush 22, Gore 193 and Nader 1.\textsuperscript{21}

\textit{Unauthorized software replacement.} Diebold (now Premier) Election Systems was caught deploying uncertified software in voting machines used in California in March 2004. The unauthorized software replacement was discovered when the machines malfunctioned. The California state government subsequently sued Diebold in September of the same year for “lying about the security of some of its equipment”.\textsuperscript{22} Diebold was caught doing the same thing in Maryland, when its machines in three counties refused to allow voters to vote for one candidate.\textsuperscript{23} ES&S similarly got caught in Indiana when a whistleblower informed local officials of the pre-election installation of unauthorized software in ES&S machines. The company was forced to pay several million dollars to settle the ensuing dispute.\textsuperscript{24}

These errors are not simply machine errors, although many are. Some are the result of human-machine and environment-machine interactions. An electronic voting machine vendor may claim error rates of less than 1 in 1.5 million ballot lines, but if the machine is transported a long distance, its may

\begin{itemize}
\item[17] Theisen, see above.
\item[18] Theisen, see above.
\item[22] Gaither, see above.
\item[24] Jeanne Cummings, see above.
\end{itemize}
need recalibration, which is not possible in the field. Or the voters may be so unfamiliar with the technology that they commit more mistakes than usual.

U.S. Federal Election Commission Standard 3.21 mandates a maximum error rate of 1 in 500,000 (2x10⁻⁶) voting positions during the testing process.²⁵ The later 2005 Standard requires error rates of “no more than one in 10,000,000 ballot positions” (10⁻⁷ or 0.00001%).²⁶ Some U.S. states, possibly anticipating that human-machine and environment-machine interactions tend to raise error rates, have adopted this stricter standard.²⁷ However, electronic voting machines in use invariably exceed these error rates, according to a research by Helen Theisen, who provides the following error rate examples below.²⁸

<table>
<thead>
<tr>
<th>System</th>
<th>Error Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal maximum</td>
<td>0.00001%</td>
</tr>
<tr>
<td>Sequoia AVC Advantage (e-vote)</td>
<td>0.68%</td>
</tr>
<tr>
<td>Sequoia AVC Advantage (e-vote)</td>
<td>0.12%</td>
</tr>
<tr>
<td>Premier (Diebold) GEMS v.1-18-24.0</td>
<td>0.08%</td>
</tr>
<tr>
<td>ES&amp;S Optech IIIP Eagle Scanner</td>
<td>0.43%</td>
</tr>
<tr>
<td>ES&amp;S Optech IIIP Eagle Scanner</td>
<td>0.10%</td>
</tr>
<tr>
<td>ES&amp;S Optech IIIP Eagle Scanner</td>
<td>0.43%</td>
</tr>
<tr>
<td>Diebold AccuVote OS Scanner</td>
<td>0.11%</td>
</tr>
<tr>
<td>Hart InterCivic Ballot Now Scanner</td>
<td>0.18%</td>
</tr>
<tr>
<td>Sequoia AVC Edge Touch Screen</td>
<td>29.49%</td>
</tr>
<tr>
<td>Sequoia Optech 4C Scanner</td>
<td>23.57%</td>
</tr>
</tbody>
</table>

According to Theisen, “all these systems are still in use in the United States”, leading her to note that “violations abound, but no federal action is taken”.²⁹

Why errors persist in voting machines

Why do such errors persist even in automated election systems? These are the possible reasons:

Software errors. No software is bug-free. Some software, after years of testing may reach a

---
²⁵ Help America Vote Act (HAVA) of 2002, Sec. 301(a)(5).
²⁸ Theisen, see above.
²⁹ Theisen, see above.
point where the bugs are well-understood, but are left untouched lest making software modifications introduce new bugs. Software of the highest quality have less than 0.1 fault per 1,000 lines of code; ordinary software may have up to 20 faults for the same size of code, even after full user-acceptance testing.\textsuperscript{30} Software bugs may result in a program stopping completely or producing senseless results. These are the easier bugs to find and to correct. Some bugs, however, may only occur at certain times and/or under certain conditions, and may manifest themselves very subtly, causing “side-effects” like small changes in variables or numbers that are not obviously noticeable. These bugs may persist for years. Some software writers are even honest enough to admit that “we wouldn’t trust the software if we wrote it ourselves”, as Eugene H. Spafford says.\textsuperscript{31} He is the executive director of the Center for Education and Research in Information Assurance and Security and a professor at Purdue University.

A classic case which occurred in 2003 is the unintentional posting in an unsecured Internet server of the source code of a Diebold touch-screen voting terminal, which a voting activist managed to download before they were taken off the Diebold FTP site. A team of experts led by John Hopkins University professor Aviel Rubin analyzed the source code and found a slew of problems, including poor software engineering practices and serious security design flaws.\textsuperscript{32}

In another case, whistleblower Daniel Spillane, former employee of the Washington D.C. voting machine vendor VoteHere who was fired by the company in 2001, claimed in 2003 that severe programming errors in the company’s electronic voting software could delete massive numbers of ballots. The company’s officials include former CIA director Robert Gates and a former senior military aide to U.S. vice-president Dick Cheney.

\textit{Hardware errors}. Some hardware problems may simply cause a machine to stop working, to work intermittently, or to issue senseless results. The more serious hardware errors may give plausible but wrong results. A common hardware source of electronic voting machine problems is miscalibration, as may happen when machines are transported over long distances, shaken, exposed to environmental stresses (see next paragraph) or as they get older. Miscalibrated machines may read the wrong names or numbers intermittently, or may assign votes to the wrong candidate, or may reject valid ballots. The first state-wide election review ever in U.S. history occurred in Hawaii in the 1998 elections, when seven of 361 electronic voting machines supplied by ES&S malfunctioned due to various causes (lens occlusion, defective cable, defective “read head”).\textsuperscript{33} Since then, voting machines have continued to malfunction on election day, causing delays, losing ballots, and disenfranchising voters.

\textsuperscript{30} Ian Brown, “Presentation on Politics and Privacy Engineering” at the Oxford Internet Institute, April 2008.
\textsuperscript{31} Gaither, see above.
Environmental stresses. Environmental stresses may cause intermittent or obscure problems that are hard to reproduce. Smudges on touch-screens, miscoloration or creases on paper ballots, mechanical stresses, high humidity, temperature extremes, and other environmental stresses may worsen slight miscalibration errors and result on false positives (reading a vote that is not there) or false negatives (missing a valid vote).

Human errors. These could be voter errors not among voters who may be unfamiliar with voting machines or with computerized equipment in general but also among the techno-savvy voting on machines which are confusing or hard to use.

U.S. election officials keep track of what is called “residual error rates”, or simply error rates, by computing the “overvotes” (where voters vote for more choices than they are allowed to) plus the “undervotes” (where voters make no valid choice at all) as a percentage of the votes cast. While this error rate tends to be an overestimate, because some undervotes are due to voters who purposely leave some ballots blank either as a protest vote or because they have no preferred candidate. Nevertheless, the relative magnitudes and changes in the error rates over different technologies and over time present a good relative measure of how prone to user error different technologies are. The best study in this regard was made by the Caltech/MIT Voting Technology Project in 2001.

A comparison of small-screen and full-face DREs also found that voter error rates were more common and reached “up to five times higher on full-face DREs [5.8% vs. 29.8% error] than on scrolling DREs.”

These human errors could also be operator or staff errors, including errors in the configuration files. In Illinois, U.S., for instance, poll operators inserted ballots or print paper improperly, causing jams and other machine breakdowns.

Poor or flawed design. These include not only the design of the hardware, the software, the data transfer mode (over networks, memory cards or flash disks), but also the screen design or ballot format.

For instance, the leaders of the expert team who, upon the request of California Secretary of State Debra Bowen, independently conducted a “top-to-bottom review” of the voting systems that California had certified, wrote: “The systems appeared not to be designed or implemented with security in mind. The design and implementation ignored basic security principles, and we found serious security vulnerabilities in all three vendors' systems. The security flaws were systemic and surprisingly similar across the three systems” They also noted that “federal testing repeatedly failed to detect these

35 Cummings, see above.
flaws in voting systems.\footnote{Matt Bishop and David Wagner, “Risks of E-Voting”, \textit{Communications of the ACM Vol. 50 No. 11}, Nov. 2007, p. 120.}

Studies as well as voter experiences have shown that even the way the ballot is presented on the screen, which is often programmed in the field, can have a major impact not only on user errors, but also on user choices – and therefore election results.

A careful study of the 2006 midterm elections in Florida’s 13\textsuperscript{th} Congressional District, for instance, where Republican candidate Vern Buchanan won over Democratic candidate Christine Jennings by 369 votes, with around 18,000 votes lost in the voting machines, concluded that “had Sarasota County used a ballot format akin to those in neighboring counties, Jennings would have beaten Buchanan.”\footnote{Laurin Frisina, Michael Herron, James Honaker and Jeffrey Lewis, “Ballot Formats, Touchscreens, and Undervotes: A Study of the 2006 Midterm Elections in Florida”, \textit{Election Law Journal Vol. 7 No. 1} (2008), p. 41.} The authors of the study assert that “ballot formats can affect vote counts in a dramatic way and, as the Florida CD-13 contest illustrates, they can be pivotal to election outcomes.”\footnote{Frisina et al., see above, p. 41.} Because the Florida machines were DREs with no paper audit trails, a recount was impossible.

When Jennings sued to open the voting machine source code for further investigation, Diebold refused and the courts agreed.

\textit{Malicious tampering}. The reasons why even seemingly minor errors should be thoroughly investigated is that these errors may simply be the tip of an iceberg. Fraudsters often hide behind clerical mistakes and “unintentional error” is a very common alibi of cheats when they are found out. Cheats may find a way to introduce an intentional bias into machines through confusing layouts, rogue code, etc. This may include inducing machine errors and/or failures in areas where their opponent is strong.

The famous “hanging chads” of Florida in the 2000 U.S. presidential elections, according to an investigative report by Dan Rather, were intentionally caused by the use of sub-standard stock for the punch cards.\footnote{“Dan Rather Reports: The Trouble With Touch Screens”, Aug. 16, 2007, http://election-reform.org/dan_rather.html}

To prove the electronic voting machines were prone to malicious tampering, Bev Harris of Black Box Voting engaged some hackers who, working with Diebold DREs, showed how to use scripts written like Trojan Horse viruses to manipulate the system's central tabulating machines, how to gain wireless access to voting machines, how to switch votes in multi-lingual voting machines, and how to hack memory cards.\footnote{Laurie Rowell, “Down for the Count”, Mar. 2008, p. 18.}
Another team of experts at the Voting Technology Research Center of the Department of Computer Science in the University of Connecticut have also shown how optical scanners could be tampered with, in a way that biases the machine, “misrepresents the counts”, and is “undetectable by pre-election tests”. Their target scanner, a Diebold Accuvote Optical Scan voting terminal (AV-OS), is “currently in wide deployment anticipating the 2008 Presidential elections” in the U.S.\(^\text{41}\)

Other demonstrations of malicious tampering include the Hursti attack\(^\text{42, 43}\) and the Princeton group’s Diebold virus.\(^\text{44}\)

**Hiding errors through trade secret protection**

The accidental release to the public of the Diebold source code gave computer security experts a revealing peek into the poor quality of electronic voting software. Diebold claimed in response that the software was an “old version”. Yet, electronic voting machine vendors refuse to release their source code for public review, claiming “trade secret protection”, in effect preventing the public and public-interest advocates from evaluating the quality of their code. For instance, when a losing candidate questioned the results of the Palm Beach City Council elections in Florida, U.S. in March 2003 and asked for a chance to inspect the voting machines, the vendor Sequoia cited its trade secret rights and refused the request for inspection. The judge took Sequoia’s side.\(^\text{45}\)

**Computer security experts distrust voting machines**

Because of the persistent errors among various electronic voting machines, around 2,000 academics and technical experts have signed a petition saying that the machines were “inherently subject to programming error, equipment malfunction and malicious tampering”.

The Association for Computing Machinery (ACM) has also adopted a “Resolution on Electronic Voting” calling for a voter-verifiable audit trail, which has been signed by more than 900 members.

---


\(^{45}\) Jason Leopold, see above.
including leading computer science researchers, computer security specialists and election automation experts.\textsuperscript{46}

A subsequent ACM “Statement on Voting Systems” made a sweeping indictment of electronic voting in general: “Virtually all voting systems in use today (punch-cards, level machines, hand-counted paper ballots, among others) are subject to fraud and error, including electronic voting systems, which are not without their own risks and vulnerabilities. In particular, many electronic voting systems have been evaluated by independent, generally recognized experts and have been found to be poorly designed; developed using inferior software engineering processes' designed without (or with very limited) external audit capabilities' intended for operation without obvious protective measures' and deployed without rigorous, scientifically designed testing.”\textsuperscript{47}

A survey by the Ponemon Institute of the Carnegie Mellon University of 100 participants at two hacking/security conferences (Black Hat and Defcon) gave the following results:\textsuperscript{48} the views of 60% of the attendees towards electronic voting were unfavorable, mainly due to concerns about programming errors (20%), attempts to influence election outcomes (17%), and potential security breaches by hackers and cyber-criminals (15%). In contrast, a parallel survey conducted by the Institute among the public (2,933 respondents) found that 55% of the public had favorable views about electronic voting. The public were more concerned about electronic voting causing a lower turnout (18%), human errors (15%), and privacy violations (15%). The Institute found the differences between expert and public opinions “startling”. Apparently, in 2004, the U.S. public has not caught up yet with security and computer experts’ concerns about persistent errors and security weaknesses in electronic voting systems.

**Fraud investigations**

Election officials as well as electronic voting machine vendors have come under investigation for fraud, and in at least one case in Ohio, officials have been convicted for committing fraud in the context of an automated election.

**Diebold.** This company has been sued for installing unauthorized software in the voting machines they fielded in the 2004 U.S. elections. In Ohio, it was sued by a law firm for selling voting machines of inferior quality and condition.

\begin{flushright}
\end{flushright}
ES&S. This voting machine vendor was sued by California Secretary of State Debra Bowen for “allegedly selling nearly 1,000 uncertified machines to San Francisco and four other counties.” According to Bowen, “ES&S ignored the law over and over and over again, and it got caught.”

Hart InterCivic. A federal suit was filed against this vendor in 2008 allegedly for “dozens of false claims and fraudulent activities… in order to receive federal Help America Vote Act (HAVA) money.

Sequoia Voting Systems. According to author Jason Leopold, “Sequoia has a history of involvement with government corruption, including the alleged pay-off of Louisiana election official Jerry Fowler.” According to another report, Sequoia regional sales manager Philip Foster was indicted in 2001 by a Louisiana grand jury for “conspiracy to commit money laundering and malfeasance… he participated in kickbacks with a Louisiana election official [Jerry Fowler] who oversaw the purchase of Sequoia equipment and is now serving a prison term.”

Smartmatic. The company was investigated in 2006 to determine whether it “paid bribes to win a Venezuela election contract in 2004“. To avoid further U.S. government investigation, the company eventually sold the U.S. voting machine company which it owned, the Sequoia Voting Systems, Inc. Yet, persistent doubts remain if Sequoia today is total free from any links with Smartmatic.

It is ironic that countries are entrusting a fundamental democratic process that demands the utmost in integrity and honesty to vendors who are suspected of involvement in shady deals and dishonest transactions.

Conclusion

---

The most common election problems under electronic voting systems are related to voter turnout. This family of problems alone can be used to manipulate automated elections by suppressing voter turnout in opposition areas and facilitating it in loyalist areas.

In addition, a whole range of machine-related problems can, unintentionally or otherwise, affect the results of the voting and potentially change the outcome of an election. The issue is magnified because a software problem, whether it is a programming mistake or malicious code, can affect thousands of machines at the same time, making it possible for one or a few individuals to influence the results even of national elections.

The current way computers are used to record, count and tabulate votes threatens the basic democratic principles of “voting in secret and counting in public”. When computers are used both to confirm a citizen’s identity and then to record the same citizen’s vote, even the threat by a person in power or fear by the public that ballot secrecy has been compromised may influence how citizens vote.

Both DREs and optical scanners were susceptible to software errors, hardware problems, environmental stresses, human errors, poor or flawed designs, and malicious tampering. DREs, however, were more problematic when they did not have paper audit trails, because recounts were impossible. Thus, even where it was clear that the automated system had gone terribly wrong, as in the case of Jennings vs. Buchanan in the 2006 congressional race for the 13th District of Florida (Sarasota County), the computer errors could not be corrected.

Even where DREs were equipped with printers that enabled voters to see audit trail printouts, it was still impossible to confirm whether the official ballot, which was invisibly stored inside memory chips or magnetic cards, truly corresponded to the printout. The only way out of this dilemma is to let voters prepare their own paper ballots, possibly aided by ballot printers, as the official document of voter intent.

Even with paper ballots, both DREs and touch-screens also showed a seemingly intractable problem: they did not count “in public”. A basketball game today can adopt electronic scoring by having a sensor on the hoop, with a computer automatically updating the score every time a ball went through the hoop. But would the fans accept such automation if they would be allowed to see the score not every time it is updated but only at the end of the game? When computers are used to keep game scores or to count votes and to consolidate totals, the electronic processes that accomplish this in silicon are totally opaque and inaccessible to ordinary citizens and even to most experts. Here is the real dilemma of current automated election designs through electronic voting – the complete loss of transparency and the exclusion of the public in the counting and consolidation of votes, which, in a real democracy, is essentially a public function.
And when votes are not counted in public, can manipulation and fraud be far behind?

The technological challenge then is to find ways to use computers in ways that enhance the capacity of the ordinary citizen to audit the electoral process in real-time, as they could easily do when votes in paper ballots were counted manually in full view of the public. To do this, the designers of automated election system need to shift their goal from “minimizing human intervention” to protecting and enhancing the principles of “voting in secret and counting in public”. Furthermore, these goals should be incorporated in the technology standards themselves, many of which, today, “seem vague, ad hoc, arbitrary and even, sometimes, unreasonable”.  

In the meantime, measures to detect and correct the mistakes that computers make, like the use of voter-prepared paper ballots, double-entry accounting in election tallies, and the mandatory post-election audit of automated election results through statistical sampling can help maintain the sanctity of the ballot.

More than a technological problem, election fraud is really a social problem and therefore calls for social solutions, supported by technological means. The only effective social solution to fraud – in elections or in any other area – is eternal vigilance and punishment for the cheats.

30 May 2008
Updated June 20, 2008

[Roberto Verzola (rverzola@gn.apc.org) is an engineer by training and is currently involved in efforts to reform the system of election tabulations in the Philippines. He is currently the secretary-general of Halalang Marangal. This article was written during his six-week research fellowship at the Oxford Internet Institute (OII) of the University of Oxford in the UK on April 21 – May 30, 2008.]

