

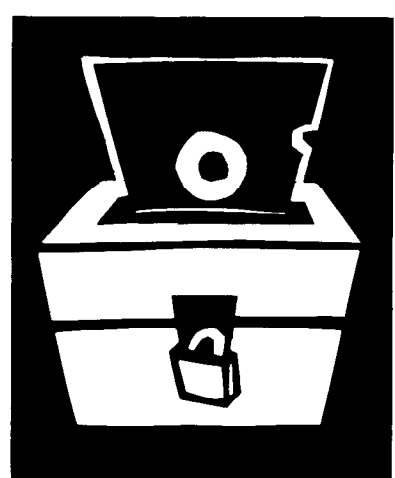
Background: Errors and alleged fraud in computer-based elections have been recurring Risks Forum themes. The state of the computing art continues to be primitive. Punch-card systems are seriously flawed and easily tampered with, and still in widespread use. Direct recording equipment is also suspect, with no ballots, no guaranteed audit trails, and no real assurances that votes cast are properly recorded and processed.

Erroneous results: Computer-related errors occur with alarming frequency in elections. Last year there were reports of uncounted votes in Toronto and doubly counted votes in Virginia and in Durham, North Carolina. Even the U.S. Congress had difficulties when 435 Representatives tallied 595 votes on a Strategic Defense Initiative measure. An election in Yonkers, N.Y. was reversed because of the presence of leftover test data that accumulated into the totals. Alabama and Georgia also reported irregularities. After a series of mishaps, Toronto has abandoned computerized elections altogether. Most of these cases were attributed to "human error" and not "computer error" (see the October "Inside Risks"), and presumably due to operators and not programmers; however, in the absence of dependable accountability, who can tell?

Fraud: If wrong results can occur accidentally, they can also happen intentionally. Rigging has been suspected in various elections, but lawsuits have been unsuccessful, particularly in the absence of incisive audit trails. In many other cases, fraud could easily have taken place. For many years in Michigan, manual system overrides were necessary to complete the processing of noncomputerized precincts, according to Lawrence Kestenbaum. The opportunities for rigging elections are manifold, including the installation of trap-

RISKS IN COMPUTERIZED ELECTIONS

Peter G. Neumann




doors and Trojan horses—child's play for vendors and knowledgeable election officials. Checks and balances are mostly placebos, and easily subverted. Incidentally, Ken Thompson's oft-cited Turing lecture, *Commun. ACM* 27, 8 (August 1984), 761–763, reminds us that tampering can occur even without any source-code changes; thus, code examination is not enough.

Discussion: The U.S. Congress has the constitutional power to set mandatory standards for federal elections, but has not yet acted. Existing standards for designing, testing, certifying, and operating computerized vote-counting systems are inadequate and voluntary, and provide few hard constraints, almost no accountability, and no independent expert evaluations. Vendors can hide behind a mask of secrecy with regard to their proprietary programs and practice, especially in the absence of controls. Poor software engineering is thus easy to hide. Local election officials are typically not sufficiently computer-literate to fully understand the risks. In many cases, the vendors run the elections.

Reactions in RISKS: John Board at Duke University expressed surprise that it took over a day for the doubling of votes to be detected in eight Durham precincts. Lorenzo Strigini reported last November on a read-ahead synchronization glitch and an operator pushing for speedier results, which together caused the computer program to declare the wrong winner in a city election in Rome, Italy. Incidentally, computerized elections are becoming more common abroad, including in a few countries notorious for past riggings. Many of us have wondered how often errors or frauds have remained undetected.

Conclusions: Providing sufficient assurances for computerized election integrity is a very difficult problem. Serious risks will always remain, and some elections will be compromised. The alternative of counting paper ballots by hand is not promising. But we must question more forcefully whether computerized elections are really worth the risks, and if so, how to impose more meaningful constraints.

Peter G. Neumann is chairman of the ACM Committee on Computers and Public Policy, moderator of the ACM Forum on Risks to the Public in the Use of Computers and Related Systems, and editor of ACM SIGSOFT's *Software Engineering Notes* (SEN). Contact risks-request@csl.sri.com for on-line receipt of RISKS. 

References

1. *New Yorker* (Nov. 7, 1988). See article by Ronnie Dugger.
2. Saltman, R.G. Accuracy, integrity, and security. *Computerized Vote-Tallying*, NIST (NBS) Special publication, 1988.
3. *SEN*, 15, 1 (Jan. 1990), 10–13, Virginia, Durham, Rome, Yonkers, and Michigan cases. Additional cases were discussed in earlier issues.

Also see publications by two nongovernmental organizations, Computer Professionals for Social Responsibility, P.O. Box 717, Palo Alto, CA, and Election Watch (a project of the Urban Policy Research Institute), 530 Paseo Miramar, Pacific Palisades, CA 20272.