



ANNALS OF DEMOCRACY

COUNTING VOTES

by Ronnie Dugger

[This article appeared as the lead article in *The New Yorker* magazine on November 7, 1988. Ronnie Dugger is the author of three books (*The Politician: the Life and Times of Lyndon Johnson*; *On Reagan: The Man and His Presidency*; *Men in Texas, Bedickek, Webb, and Dobie*). He founded the *Texas Observer* of which he was the editor. He also wrote "A Call to Citizens: Real Populists Please Stand Up!", which led to the founding of the Alliance for Democracy (www.thealliancefordemocracy.org)]

DURING the past quarter of a century, with hardly anyone noticing, the inner workings of democracy have been computerized. All our elections, from mayor to President, are counted locally, in about ten thousand five hundred political jurisdictions, and gradually, since 1964, different kinds of computer-based voting systems have been installed in town after town, city after city, county after county. This year, fifty-five per cent of all votes-seventy-five per cent in the largest jurisdictions-will be counted electronically. If ninety-five million Americans vote on Tuesday, November 8th, the decisions expressed by about fifty-two million of them will be tabulated according to rules that programmers and operators unknown to the public have fed into computers.

In many respects, this electronic conversion has seemed natural, even inevitable. Both of the old ways -- hand-counting paper ballots and relying on interlocked rotary counters to tabulate votes that are cast by pulling down levers on mechanical machines -- have been shown to be susceptible to error and fraud. On Election Night, computers can usually produce the final results faster than any other method of tabulation, and so enable local officials to please reporters on deadlines and to avoid the suspicions of fraud which long delays in counting can stimulate.

Recently, however, computerized vote-counting has engendered controversy. Do the quick-as-a-wink, computerized systems count accurately? Are they vulnerable to fraud, as well, even fraud of a much more dangerous, centralized kind? Is the most widely used computerized system, the Votomatic, which relies on computer punch-card ballots, disenfranchising hundreds of thousands of voters?

It appears that since 1980 errors and accidents have proliferated in computer-counted elections. Since 1984, the State of Illinois has tested local computerized systems by running many thousands of machine-punched mock ballots through them, rather than the few tens of test ballots that local election officials customarily use. As of the most recent tests this year, errors in the basic counting instructions in the computer programs had been found in almost a fifth of the examinations. These "tabulation-program errors" probably would not have been caught in the local jurisdictions. "I don't understand why nobody cares," Michael L. Harty, who was until recently the director of voting systems and standards for Illinois, told me last December in Springfield. "At one point, we had tabulation errors in twenty-eight per cent of the systems tested, and nobody cared."

Robert J. Naegele, who is the State of California's chief expert on certifying voting systems and is also the president of his own computer consulting firm, has been hired by the Federal Election Commission (F.E.C.) to write new voluntary national standards for computerized vote-counting equipment and programs. Last spring, in San Francisco, at a national conference of local-election officials, I asked Naegele whether computerized voting as it is now practiced in the United States is secure against fraud.

He pointed a thumb at the floor. "When we first started looking at this issue, back in the middle seventies, we found there were a lot of these systems that were vulnerable to fraud and out-and-out error," he said.

I asked him whether he regarded as adequate the typical fifty-five-ballot "logic-and-accuracy public test" that is conducted locally on the Votomatic computerized punch-card vote-counting system-which about four in ten voters will use on November 8th-and he said, "No."

Would such a test discover, for example, a "time bomb" set to start transferring a certain proportion of votes from one candidate to another at a certain time, or any other programmers' tricks?

"Of course not," Naegele said. "It's not a test of the system. It's not security!"

The old mechanical machines prevent citizens from "overvoting"-voting for more candidates in a race than they are entitled to vote for-but the Votomatic systems do not. Not only can people using these systems overvote but election workers, if they are dishonest, can punch extra holes in ballots to invalidate votes that have been correctly cast or to cast votes themselves in races the voter has skipped. In the 1984 general election, about a hundred and thirty-seven thousand out of a total of 4.7 million voters in Ohio did not cast valid ballots for President-mostly, according to Ohio's secretary of state, because of overvoting. The computerized punch-card voting system is "a barrier to exercise of the franchise," and causes "technological disenfranchisement," Neil Heighberger, the dean of the College of Social Sciences at Xavier University, in Cincinnati, concluded in a recent study he made of the subject.

A federal judge, William L. Hungate, ruling last December on a lawsuit in St. Louis, declared that the computerized punch-card voting system as it has been used in that city denies blacks an equal opportunity with whites to participate in the political process. The suit was filed by Michael V. Roberts, a black candidate for president of the Board of Aldermen who in March of last year had lost to a white by a fourth of one per cent in a city election in which voting positions on ballots in the black wards were more than three times as likely not to be counted as those in white wards. Roberts, who was joined in the suit by the St. Louis branch of the National Association for the Advancement of Colored People, contended that computerized voting is such a relatively complex process that it is tantamount to a literacy test, and literacy tests have been prohibited by federal law as an unconstitutional burden on the right to vote. Judge Hungate found that in four local elections since 1981 voting positions had not been counted by the computerized system on anywhere from four to eight of every hundred ballots in black wards, compared with about two of every hundred in white wards (and also found that in the March, 1987, election the computerized returns from six per cent of the precincts had "irreconcilable discrepancies"). The evidence indicated that the computer had passed over the uncounted positions because of either overvoting or undervoting, which is failing to cast a vote in a race. The Judge ordered officials to count by hand all ballots that contained overvotes or undervotes and to intensify voter education in the black wards, but the city appealed, arguing that the racial differential does not always hold true in the city's elections. The Missouri secretary of state, Roy Blunt, called the order to recount the ballots by hand unfair and said that it could "make punch-card voting unworkable."

In Pueblo, Colorado, in 1980, suspicions about the vote-counting on punch-card equipment led to an investigation by a computer expert, but nothing was proved. In Pennsylvania, in 1980, two of three examiners recommended that the Votomatic punch-card system marketed by Computer Election Services (C.E.S.), of Berkeley, California, be rejected, on the ground that it was fraud-prone, but the secretary of the Commonwealth of Pennsylvania approved it anyway. In Tacoma, Washington, in 1982 and 1987, in the only known local referendums on computerized voting, citizens' crusades, led by a conservative Republican, Eleanora Ballasiotes, that focused on the vulnerabilities of computers to fraud resulted each time in the voters' three-to-one rejection of the systems that their local officials were about to buy. A group of defeated Democratic candidates in Elkhart, Indiana, sued local election officials in 1983, alleging that computer-based irregularities had occurred in a 1982 election; they have since lost three lawsuits, and a fourth one continues. In Dallas, Terry Elkins, the campaign manager for Max Goldblatt, who in 1985 ran for mayor, came to believe, on the basis of a months long study of the surviving records and materials of the election, that Goldblatt had been kept out of a runoff by manipulation of the computerized voting system. The attorney general of Texas, Jim Mattox, was impressed by the charges and conducted an official investigation of them. Dallas authorities have declared that since there is no evidence of criminal behavior the case is closed, but Mattox has refused to close it. "I do not think that there were adequate explanations for the anomalies," he told me, in Austin.

COMPUTER programmers working for the private companies that sell election equipment write their programs in higher computer languages or the intermediate assembly language, and these are translated or compiled into the binary language of ones and zeros which computers understand. The original programs, which are centrally produced, are commonly called "source codes;" only a few local governments own and control the source codes that are used in their jurisdictions. According to Jack Gerbel, a founder of C.E.S., who has sold more computerized vote-counting equipment than any other individual in the country, about half the time the companies' programmers also write the codes that "localize" (or "initialize") vote-counting systems for the specific elections of each jurisdiction. The source and local codes together tell the computers how to count the votes. Local public tests may or may not adequately test the local codes, but, as Naegele said, they do not test the source codes.

The election-equipment companies, which thus both sell and program the computers that tabulate public elections, have long contended, in and out of court, that they own the source codes and must keep them secret from everyone, including the local officials who conduct elections. In 1985, Jack Kemp (no relation of the congressman), the president of C.E.S., which was then the leading election-equipment company in the country, warned in so many words that an outsider who got the company's source code could compromise elections with it. Through an affidavit that Kemp furnished for a lawsuit in

Charleston, West Virginia, the company affirmed that the security of the vote-counting in C.E.S. equipped jurisdictions depended in large measure on its retention of the secrets of the code, and that there would be "a grave risk" to this security if the defeated candidates were permitted to see the code. "The significance of the company's proprietary interest in its software is incalculable from our perspective," Kemp asserted.

That significance is incalculable from the voter's perspective, too. Insofar as source codes have not been opened to examination on behalf of the public-and most have not-instructions to computers on how to count votes appear to have become a trade secret. Only a few states have demanded copies of the source codes, and only in the last year or two have any states examined them. Thus most of the local officials who preside over computerized elections do not actually know how their systems are counting the votes, and when they officially certify that the election results are correct they do not and cannot really know them to be so.

After systems that use computer punch cards as ballots have counted the votes, manual recounts of the holes in the punch cards can be demanded, provided the cards have not yet been destroyed by local officials-as is permitted by most local laws after a specified period of time. But in a new computerized system, "direct-recording electronic" (D.R.E.), which is becoming more widespread, there are no individual ballots, and, the way these new machines are now being used in many jurisdictions, recounts are impossible, for the program destroys the electronic record of each voter's choices the instant after it counts them.

The dominant company now in the sale and programming of computerized vote-counting systems for public elections, Cronus Industries, of Dallas, is better known as its sole and wholly owned subsidiary, the Business Records Corporation (B.R.C.). Cronus/ B.R.C. has accused the R. F. Shoup Company, of Bryn Mawr, Pennsylvania-one of its rivals for a forty-million-dollar voting-equipment order from New York City-of infringing B.R.C. patents in the very D.R.E. vote-counting machine, the Shouptronic, that Shoup is trying to sell to New York. In a lawsuit filed last November in Philadelphia, Cronus, on whose equipment between thirty and forty-five million votes will be counted this year, has also sought to discredit Shoup, on the basis of a 1979 conviction of Ransom Shoup II, the president of the company, of two federal felonies-conspiracy and obstruction of justice-in connection with an F.B.I. investigation of an election in Philadelphia that had been counted on mechanical-lever machines. For these offenses, Ransom Shoup was fined ten thousand dollars and given a three-year suspended sentence. Counterattacking, the Shoup firm, whose equipment will tabulate an estimated million and a half votes on November 8th, has accused Cronus of reaching for "a virtual monopoly on the entire business of supplying voting equipment for use in political elections in the United States" and has alleged that the Cronus vote-counting systems that are in use "inherently facilitate the opportunity for various ... forms of fraud" and "create new and unique opportunities for fraudulent and extremely difficult-to-detect manipulation and alterations with respect to election results."

In 1985 and 1986, Cronus bought Computer Election Systems and also eight smaller election-equipment and election-printing firms, while selling off three other subsidiaries, thereby transforming itself, in eighteen months, from a small conglomerate of disparate industrial businesses into the titan of the computerized-vote-counting business.

Cronus is now responsible for most C.E.S. systems that are still in service and for a computer-based "mark-sense" voting system that B.R.C. has sold in the past few years. B.R.C. also sells computerized voter-registration systems; election supplies, including, this year, perhaps a hundred and sixty million punch-card ballots; election assistance and service; and other computerized information services for local governments. C.E.S. used to take pride in publicizing the millions of votes cast on its machines (a total of three hundred and fifty million between 1964 and 1984), and after Cronus bought C.E.S., in 1985, C. A. Rundell, Jr., then the chairman and chief executive officer of Cronus, told a reporter that his company had about forty per cent of the election-service market. But when I asked Rundell earlier this year how many votes Cronus systems will count in 1988 and in which jurisdictions, he refused to say. "We certainly are not going to provide you with a list of customers and the kinds of systems they have," he declared. "We've got to ask how much competitive intelligence we divulge to our competition." He did volunteer that the total for votes counted by Cronus systems was below thirty-five million. Officials at R. F. Shoup, however, seeking to prove that Cronus is a monopoly, charge that Cronus systems will count fifty or sixty million votes on November 8th. In any case, Cronus and C.E.S. systems are used by the voters in such cities as Los Angeles, Chicago, Detroit, Houston, Phoenix, Miami, Seattle, Minneapolis, Cincinnati, and Cleveland.

On Election Day, about one in every three American voters still pulls down the lever on an old thousand-pound mechanical-lever machine, and about one in every nine still marks the old-fashioned paper ballot that is counted by hand. In the past two years, however, more than eighty United States counties have abandoned lever machines, and more than ninety have abandoned paper ballots, the replacements being in most cases either D.R.E. or mark-sense systems. In mark-sense systems, which are also called "optical-scan," computers employing light or electrical conductivity count votes that have been cast on ballots with pencils or markers. Mark-sense is now used by about eight per cent of the voters; a multi-punch-

card, count-the-holes computer system called Datavote, which is sold by Sequoia Pacific Systems Corporation, of Exeter, California, is used by about four per cent; and electronic D.R.E. systems, the newest computerized voting technology, are used by about three per cent. "The election business is shifting into the mark-sense and the electronic [D.R.E.] stuff," according to Richard J. Stephens, the president of a small election company in Escondido, California, who has been in the field since 1966. "The punch-card systems will remain out there, but B.R.C. is not trying to sell punch-card anymore-it's selling mark-sense now."

THE private business of counting votes in public elections can be realistically understood only as a small, if extremely important, segment of the computer industry itself, and thus a business that has both the strengths and the weaknesses of the over-all industry. The computer industry's strengths-astoundingly vast and rapid computational power, the automation of trillions of transactions have been well known for some time, but the weaknesses have come to be understood only lately. In recent years, the vulnerability of computers to tampering and fraud has become a commonplace in many industries. Computer operators do not leave fingerprints inside a computer, the events that occur inside it cannot be seen, and its records, and printouts can be fixed to give no hint of whichever of its operations an operator wants to keep secret. The practical problem of the computer age is invisibility. Hackers-adventurous programmers-penetrate corporate and governmental computers for fun and jimmy the programs in them for gain. "Electronic cat burglars" have stolen billions of dollars from banks and other businesses-a billion a year by a recent estimate of the American Bar Association. By means of computer fraud employees have raised their salaries and students have raised their grades. Caltech students printed out more than a million entry blanks for a McDonald's contest and won a Datsun station wagon. Employees of a federal agency diverted tens of thousands of dollars to nonexistent employees. In the infamous 1973 Equity Funding Corporation fraud, company officials and other employees typed into their computers names of about sixty-four thousand people who didn't exist as holders of more than two billion dollars' worth of life-insurance policies that didn't exist but were "resold" to reinsurers. "Electronic dead souls," the writer Thomas Whiteside has called these fabricated customers.

Whether or not elections have ever been stolen by computer before, some citizens and some officials are asking if it could happen in the future. Could a local or state office or a seat in the United States House of Representatives be stolen by computer? Might the outcome of a close race for a United States Senate seat be determined by computer fraud in large local jurisdictions? Since, under the state-by-state, winner-take-all rules of the electoral college, a close Presidential election can be decided by relatively few votes in two or three big states, could electronic illusionists steal the Presidency by fixing the vote-counting computers in just four or five major metropolitan areas? Could people breaking into or properly positioned within a computerized-vote counting company, acting for political reasons or personal gain, steal House or Senate seats, or even the White House itself?

Randall H. Erben, the assistant secretary of state in Texas, who served as special counsel on ballot integrity to President Ronald Reagan's campaign in 1984 and, in 1986, headed a similar group for Governor Bill Clements, of Texas, told me in Austin, "I have no question that somebody who's smart enough with a computer could probably rig it to mistabulate. Whether that has happened yet I don't know. It's going to be virtually undetectable if it's done correctly, and that's what concerns me about it." Willis Ware, a Rand Corporation computer specialist, warned those attending a 1987 conference on the security of computer-tabulated elections, "There is probably a Chernobyl or a Three Mile Island waiting to happen in some election, just as a Richter 8 earthquake is waiting to happen in California." The chief counsel of the Republican National Committee, Mark Braden, told me that he has yet to see a proved case of computer-based election fraud, but added, "People who work for us who know about computers claim that you could do it."

Some officials concerned with elections think about the unthinkable in their field; namely, the stealing of a Presidential election by computer fraud in the vote-counting in metropolitan areas of key states. Steve White, the chief assistant attorney general of California, said to me last spring in Sacramento, "It could be done relatively easily by somebody who didn't necessarily have to be all that sophisticated. Given the importance of the national election, sooner or later it will be attempted. There is a real reluctance to concede the gravity of the problem."

Jim Mattox, the Texas attorney general, while discussing Cronus/B.R.C./ C.E.S., exclaimed to me in dismay a year ago, "One thing is clear: one company in the United States should not have as big an impact on elections as this company has got. Nobody should have in a democracy. The right to vote is too sacred."

COMPUTERS can be ordered to transfer votes from one candidate to another, to add votes to a candidate's total, to determine an outcome in accordance with a specified percentage spread. All the computer experts I have spoken with agreed that no computer program can be made completely secure against fraud. Where they differed was in their characterizations of this fact. Local election officials and election equipment-company specialists, executives, and salesmen usually took the position that state certification procedures and local logic-and-accuracy tests provide enough security for

-----|

reasonable assurance that elections are honestly counted. The independent computer specialists I interviewed were divided, generally speaking, into two camps. One, led by Roy Saltman, of the National Bureau of Standards, Robert Naegele, and Lance Hoffman, of George Washington University, sees local-election theft by computer as possible, but stresses the fact that no case of program tampering has been proved. This camp attributes the manifold problems of computerized vote-counting entirely or almost entirely to inadequacies in the administration of elections and insufficient testing of the equipment, and regards the theft of the Presidency by computer as, in effect, impossible. The other, led by the Pennsylvania voting-systems examiner Michael Shamos and the computer specialists Howard Jay Strauss, of Princeton, and Peter G. Neumann, of S.R.I. International, a nonprofit research institution in Menlo Park, California, emphasizes the ease of concealing theft by computer "without a trace;" characterizes local elections as very vulnerable to fraud; and regards the theft of the Presidency by computer as entirely possible.

Should citizens delegate the job of vote-counting to technicians? Most people do not know enough about computers to be able to tell what is happening during computerized vote-counting, even if they are looking straight at the card readers and computers. In Dallas last year, during a conference of citizens concerned about this issue, David T. Stutsman, an Indiana attorney with experience in contested-election cases, said, "In traditional elections, the people in your neighborhood, your neighbors, had the responsibility and the legal duty to supervise an election. They counted the votes. The precinct officials don't count the votes anymore. The power-that is, political power-has gone to the vendors, to the vendors' representatives, and to the people that operate those machines." He also said, "You're putting more power in the hands of fewer people."

Demands for much stricter security in computerized elections appear to be gaining adherents in many quarters. Sometime after the November election, results the National Clearinghouse on Election Administration, a grandly named four-person office in the F.E.C., will publish voluntary, but potentially influential, national standards for the security and accuracy of computerized elections. In a late-summer draft, the Clearinghouse proposed that the election-equipment companies place their source codes in escrow, the idea probably being that in the event of seriously disputed election results the codes could be obtained and examined by representative's of the public.

THE evolution from counting paper ballots one at a time to counting as many as a thousand punch-card ballots a minute occupied about seventy years-a period that can be seen as having opened in 1892, when lever voting machines first appeared. Four years later, Joseph P. Harris, the inventor of the Votomatic system, was born, on a farm in North Carolina. In the First World War, Harris was a flying instructor, and afterward he helped pay for his doctorate in political science at the University of Chicago by flying the mail between Chicago and Cleveland in open-cockpit planes. A favored student of Charles Merriam, who was seeking to develop a scientific basis for understanding politics, Harris became a teacher and a scholar who over four decades wrote many books on politics and elections. He refined and championed the process of permanent voter registration, and it was largely through his efforts that permanent registration replaced the earlier system of recurring reregistration. In the nine-teen-thirties, drawn to Washington by the New Deal, he served on committees advising President Roosevelt on economic-security and administrative management issues.

Early in his career, Harris saw for himself that the politicians in big cities stole votes easily. Touring voting places during a Chicago election in the nineteen-twenties, he spotted a shotgun at one precinct and also noted "a good deal of corruption that you could see." In a 1934 book, "Election Administration," he recounted the details of proved ballot-stuffing, repeat votes cast by paid drunks (sometimes fifteen or twenty times), and shameless miscounting in Philadelphia, Pittsburgh, and Cleveland, and he quoted Boss Tweed's testimony before the Board of Aldermen in New York City that he had routinely instructed his Tammany Hall men to "count the ballots in bulk, or without counting them announce the result in bulk, or change from one to the other, as the case may have been," and Tweed's further statements that "the ballots made no result; the counters made the result," and "I don't think there was ever a fair or honest election in the City of New York." During several summers in the nineteen-twenties, Harris supervised the installation of lever voting machines made by the Automatic Voting Machine Company, of Jamestown, New York (he gave up the job with A.V.M. because he felt that it tainted him somehow). He was struck by the machines' complexity, weight, and cost, but he also realized that the lever machines represented a big step forward in a long process. People had voted with kernels of corn or black and white beans in Massachusetts in the sixteen-forties, viva voce or by a show of hands in pre-Revolutionary times, and on paper ballots that they wrote out for themselves or had written out for them, then on printed ones, then on the secret and official printed "Australian" ballots that were adopted generally in the second half of the nineteenth century. When a voter using the mechanical machine presses down a lever beside a printed choice, the return of the lever to its original position causes a tenth of a turn on a tens counter, which is connected to a hundreds counter. A.V.M. was the first large firm in the field. Samuel R. Shoup, the grandfather of the president of the present R. F. Shoup Company, organized the principal rival to A.V.M., the Shoup Voting Machine Corporation (S.V.M.), in 1905.

By 1928, a lever machine was used by about one of every six American voters. In the early thirties, while he was a

professor of political science at the University of Washington, Harris began to have constructed in the university's engineering shops a gizmo that he thought of as the application of the principle of the player piano to the mechanical voting machine. ("The computer was beyond my dreams," he said later.) One voted on Harris's device by depressing keys that made perforations in a paper roll, and in due course the machine would automatically count the perforations and print the results. A Seattle businessman went halves on it with Harris, and in 1934, after much difficulty, the moonlighting professor won a patent, but by then he understood that financially the project was far beyond him and his friends. He invited "the I.B.M.," as he called the International Business Machines Corporation, to develop and market his device, but, in 1937, the company turned him down. On the eve of the Second World War, he was still tinkering with the machine-considering entering votes on the paper roll as lead marks that could be read electrically, or even, as he wrote to I.B.M.'s director for market research in 1939, "on a punch card."

For Harris, as for nearly everyone, the war intervened, and he taught management and administration at a school for military officers. One day in the early nineteen-sixties, though, when he was teaching at the University of California at Berkeley, a former student asked him if he had ever thought of using a standard I.B.M. computer punch card for vote-recording. "I hadn't, but I did," Harris wrote later; he had forgotten his own idea of 1939. Soon after he had been asked about the I.B.M. card, the election chief of Alameda County, California, complained to him that the lever voting machines could barely handle the current ballots, which kept growing longer. "Joe," he said, "what we need is some kind of a simple mechanical device that can be related some way to a computer." In that context, the election official talked about the I.B.M. Port-a-Punch, a hand-held device for punching out the rectangles on the I.B.M. card. "I started to think," Harris said later. After a cataract operation in 1962, as he lay bedridden for two weeks with pads taped over his eyes, he had a eureka experience: he suddenly visualized "a computer card in an inexpensive holder with a permanent election 'book' pre-marked with candidates and issues."

The founding president of C.E.S., Robert P. Varni, told me what happened next. We were in his apartment in San Francisco, a twenty-third-floor Nob Hill penthouse looking out across the great sweep of the bay, the islands, and the bridges. "I was working for I.B.M.," he said. "One of my accounts was U.C. Berkeley. I got a call from Joe Harris. He asked about the I.B.M. Port-a-Punch. 'I have an idea, and I'd like to borrow it for a while,' he said. He didn't want to buy it. It was an eight-dollar item. He wanted to borrow it, along with about a dollar and a half's worth of punch cards."

Assisted by William S. Rouverol, a retired professor, who was an engineer, Harris cobbled together his ingenious new device for computerized vote counting. "After a while," Varni went on, "he called and said, 'I've done something interesting with that Port-a-Punch you lent me.' I went to his office and he showed me the first prototype of the Votomatic." Harris said later that he had derived the name of his invention from the Shine-O-Matic, a shoeshine machine he had read about in the Sunday paper.

Varni is now the trim, prosperous chairman of a firm that computerizes police and fire departments. As he recalled those early days, he often broke into a warm smile. Harris didn't know anything about computers and needed someone who did, so, in 1963, Varni sent him to Kenneth Hazlett, an athletic young man who was the foreman of the university's computer room. Hazlett had had only two years of higher education, at Oakland City College, but he had been introduced to tabulating machines during a two-year spell in the Navy, and after taking an I.B.M. course in programming he had begun teaching the skill to some of his staff at Berkeley.

"Joe Harris walked into my office with a handful of these Port-a-Punch cards and wanted to know if they'd go through a computer," Hazlett recalled. "I walked him outside my office to a small I.B.M. computer, and from the console I keyed in about a three instruction loop that would simply flush these cards through the card reader. And they went sailing through. Joe Harris just lit up!" Harris realized that he could use the cards themselves as ballots. He showed Hazlett a mockup of the prototype, and, Hazlett said, "I agreed to do him a real program." To produce and sell his invention, Harris then formed Harris Votomatic, Inc., with a quarter of a million dollars he raised from about two dozen of his colleagues at the university, including Hazlett, and from Varni. Having retired from teaching, he then began driving around the West trying to sell his invention.

Devising the early programs for what became the C.E.S. systems, Hazlett gave next to no attention to security against the kinds of fraud that could be concealed in the computerized system itself. "There are two problems," he told me last spring in his sunlit apartment in Corvallis, Oregon. "One is getting the system to work the way you want it to, and the other problem is avoiding fraud. We concentrated mainly on the first. Then, beyond that, we worked with county and state governments, cooperated in developing procedures for logic-and-accuracy-testing programs -which is running ballot cards having known votes through and verifying the totals that are produced, and even the counting by hand or machine of selected precincts post-election to look for fraud or error. And that's about all we can do."

Does Hazlett have confidence now in the security of computerized elections against fraud?

"Not a hundred per cent," he said. However, he added, he knew of no elections that had been stolen by computer.

Is a logic-and-accuracy test actually a test of a system's accuracy? "Obviously it isn't as far as you could go in testing the program," Hazlett said. "It's a very simple test. If a programmer had the necessary programming tools, he or she could get around that kind of test-of course. Knowing that the deck is fifty-five cards, you could trigger some function to come into service after fifty-five cards. Use your imagination-there are any number of things you could do. It's not an easy problem."

According to Donald G. Baumer, an engineer who worked with Hazlett, both of them realized that the Votomatic counting system could be manipulated-for instance, through the toggle switches that were on the front of a Data General Nova computer -but it was assumed that nobody would do this, because anybody who tried it could be seen. In the workshop at his small election-equipment company, near San Francisco, Baumer explained, "The concept was to devise a program that no one could ever get to - you would have to be a knowledgeable person, you would have to have the source code, and you would be very visible, standing in front of a computer throwing switches."

As Harris got older, he realized that he could not wheel around the country selling Votomatics forever. Managers who were looking for new products had taken over Varni's unit at I.B.M., and in 1965-Varni having disclosed his investment-I.B.M. bought the assets and patents of the Harris Votomatic and became for four years the nation's principal computerized-election-equipment company. Harris served I.B.M. as a paid consultant throughout the period.

"Glitches"-the term that company people seem to prefer for errors and accidents in computer elections-began to emerge in those earliest years. For example, in May, 1968, in Klamath County, Oregon, candidates' positions on the ballots were rotated in the precincts to avoid giving any candidate the unfair advantage of the top position everywhere, but the ballots got mixed up, and voters in more than a fourth of the precincts punched out rectangles for candidates they did not mean to vote for. Harris said later that as the new system became controversial, I.B.M. responded in some communities "by instructing its staff to describe the machine as the Harris Votomatic," not I.B.M.'s.

In Los Angeles County in the June, 1968, Presidential primary, deputy sheriffs were to carry voted punch cards from the precincts to two regional counting centers-one on Third Street, and the other at the I.B.M. Service Bureau Corporation, on Wilshire Boulevard, next door to the Ambassador Hotel. However, after Senator Robert F. Kennedy was shot that night at the Ambassador, police cordoned off a four-block area around the scene, and the tapes containing the totals from the Third Street center could not be brought into the I.B.M. building. The counting was not completed until nine o'clock the next morning. Reporters were irritated by the delay, and officials at I.B.M. began to wonder seriously about the risks of the election business, which, comparatively speaking, was providing only a small profit.

That November, in Missoula County, Montana, in the national contest between Hubert Humphrey and Richard Nixon, another difficulty arose. Joseph H. Chowning, who was an I.B.M. salesman then, told me not long ago, "Through a programming error in a few precincts, ballots cast for Nixon were counted for Humphrey or vice versa." In traditional Republican strongholds, Nixon was defeated, while Democratic redoubts went for him. In a precinct where both paper and punchcard ballots were used, Nixon swept the paper ballots, but the computer voted for Humphrey by a landslide. The error was caught immediately, Chowning said, but he and an I.B.M. publicrelations man had to fly to Missoula to dispel the unease.

One other event, a singular one, came to Chowning's attention about this time. "Just before or after the 1968 election, there was an article or editorial in a small suburban Chicago newspaper that came out and said that the reason I.B.M. was in the business was to make Thomas Watson President of the United States," he recalled, referring to the chairman of I.B.M. "I'm guessing, but I'm sure it went right straight to Mr. Watson's desk." Ken Hazlett, too, has a vague memory of this. "I wondered at the time if T. J. Watson was interested in running for President," he told me.

Chowning went on, "Here I.B.M. had a product that guaranteed two or three per cent of its gross income and eighty to ninety per cent of its publicity, not all of it favorable." I.B.M. got out of the vote-counting business. By 1969, it had licensed five voting equipment companies to sell the Votomatic: two in Illinois, one in New York, one in Tulsa, and C.E.S., which was founded by Varni and three other I.B.M. men-Chowning, Jack Gerbel, and Ken Hazlett (whom I.B.M. had hired to write programs for the Votomatic)-and which therefore had the great advantage of its executives' association with I.B.M.'s reputation.

Varni and his team at C.E.S. had a good run. By 1976, nearly seventeen million voters-more than a fifth of all those voting for President that year-entrusted their election decisions to C.E.S. counting systems.

The C.E.S. Votomatic punch-card system "has probably had more effect on the country than almost any other product," Varni said to me. Although today it is generally regarded as an outmoded technology, it is by far the most widely used method of counting votes by computer. The Votomatic is based on the assignment of a tiny, numbered pre-perforated rectangle on a standard eighty-column, twelve-row I.B.M. punch card to each candidate and the assignment of other rectangles to the "yes" and "no" positions on each question to be voted on. This punch card, covered with numbers but displaying no names of candidates and none of the propositions to be voted on, is the ballot. The vote recorder, which is the Votomatic, is a spined booklet listing the choices of the day in writing and mounted over a plastic mask that is designed to prevent voters from punching out any holes but the ones they are supposed to be able to punch. The voter slides the punch card underneath the booklet and then fits two holes near the top of the card onto two posts that are intended to keep the card properly aligned under the booklet. Alongside the choices printed on each page, arrows point to holes that match numbered rectangles on the underlying card. The voter turns the pages and, using a simple stylus attached to the device by a chain, punches out the rectangles that, as holes in the punch card, express his or her choices.

After the polls close, stacks of the voted punch cards are fed into card readers, in each precinct or in one central counting place, depending on the preference of the officials of the jurisdiction. A blower in each reader creates an air-stream and fluffs up some of the cards at the bottom of the stack; a pump creates a vacuum; and a spinning cylinder attached to the pump seizes a ballot and flings it past a light whose beam flicks through each punched-out hole, the cards whizzing through the reader at a rate of up to a thousand a minute. If the spinning cylinder doesn't grab two ballots at a time, if the minute punched-out rectangles of cardboard have separated properly from the cards, and if the computer underneath and connected to the card reader has been programmed correctly, the computer then quickly and accurately tabulates the votes; that is, it counts according to its location each pinpoint of light that twinkles through a card for a millisecond.

The punched-out scraps, which have come to be called "chad," are supposed to be forced between two vertical rubber strips underneath the ballot and into a chad box. Sometimes, however, a chad does not break completely free from the card and becomes a "hanging chad," and sometimes voting-hole rectangles are merely indented by the voter's stylus. "Hanging chad has been with us since the invention of the Votomatic," Hazlett told me. C. A. Rundell, of Cronus, informed me during an interview in his office in Dallas last fall that because of the chad problem, and also because of wear and tear on the ballots, vote totals may not change the first time ballots are run through the card reader, and probably won't the second time, but the third or fourth time they may change, "and then you've lost your audit trail." The inexact science of divining what the voter intended in the case of a mere indentation or whether the card reader counted a hole that was partly or wholly blocked by a hanging chad has been called "chadology."

Presumably, most of the elections counted by the C.E.S. systems went smoothly ("People don't want to read about a good election," Jack Gerbel told me in September), but the company did have problems. In the 1970 primary in Los Angeles, voters in some precincts voted for the wrong candidates because of incorrect rotations; in other precincts ballot pages were missing. A computer program did not record totals on a hundred of its counters. Ballot cards jammed in the card readers and had to be duplicated by election workers-clerks were seen poking holes in punch cards with pencils. The central computer stopped or was stopped six times during the counting; and it was discovered only after the counting that more than five hundred precincts had been overlooked.

In 1970, the election commissioners in St. Louis, who were considering buying the Votomatic system, asked the accounting firm Price Waterhouse to evaluate it, with devastating results. Security controls on the Votomatic would be "more easily subject to abuse" than those on the mechanical machines in place, the firm said. Candidates' names could be misaligned with the rectangles on the ballot "by manipulation of the ballot book pages' printing or positioning, by manipulating the positioning of the punched card used to record the vote, or by manipulation of the program used to tabulate the vote," the report continued. "It is possible to write a program in such a way that no test can be made to assure that the program works the way it is supposed to work.... It is possible to set card readers to misread the information punched into the cards. It is possible to have instructions in computer memory to call in special procedures from core, tape, or disk files to create results other than those anticipated. . . . There is no practical way to assure accuracy of the proposed computer tabulation short of complete duplicate processing on third party computers with reproduced ballot card decks and third party control programs." Gerbel, who was taking over the C.E.S. sales effort in major jurisdictions, responded with a long recitation of the customary tests and safeguards, and also emphasized the system's acceptance in fifteen states, discounted "information supplied by competitors," and concluded, "For six years, the personnel of C.E.S. have answered the comments made in this report by conducting successful Votomatic elections."

IN 1977, C.E.S. was bought out by Hale Brothers Associates, a San Francisco investment company controlled by Prentis Cobb Hale, Jr. When his family acquired C.E.S., through a "friendly cash offer," for twelve million dollars, Prentis Hale, an influential Republican who was given to partridge-hunting with General Franco in Spain, was best known as the Hale in Carter Hawley Hale (C.H.H.) -the nation's seventh-ranking chain of department stores and the largest chain in the West. The year Hale bought the election company, C.H.H. earned fifty million dollars on sales of a billion and a half dollars.

A couple of years later, C.E.S. survived an investigation by the antitrust division of the justice Department. "We became the target of a criminal grand jury," David L. Dunbar, the company's president at that time, told me recently. The investigation lasted more than a year, and the company turned over a whole file cabinet of records to the justice Department. The investigation was dropped very early in 1981-in January or February, Dunbar recalled, adding, "I used to kid people we had to get Ronald Reagan elected to get this thing killed."

As the eighties opened, C.E.S. was the unchallenged leader in the business of computerized vote-counting equipment. In 1980, C.E.S. systems were in place where about thirty-five million Americans were registered to vote, and they counted about three out of ten of the votes that were cast in the United States. Two years later, C.E.S. equipment tallied thirty-six per cent of the votes in the country. As of November 6, 1984, nine out of twenty votes, 44.2 per cent-were counted on C.E.S. equipment in a thousand and nineteen jurisdictions in forty states. To put this a different way, the electronic technology made and marketed by one small company housed in an industrial building near San Francisco Bay counted the votes that were cast in more than sixty-four thousand precincts where almost forty-seven million Americans were registered to vote.

The period 1977 through 1986, when C.E.S. for the most part dominated the computerized-election business, was a time of technical mishaps and rising suspicion. A precursor of the serious breakdowns that lay ahead had occurred in a legislative race in Los Angeles in 1976. The outcome was reversed twice-once by a machine recount, the second time by holding every one of the hundred thousand ballots up to a light and counting the holes one by one. "Hanging chad" and "bulging chad," as the indented tabs were sometimes called, were blamed for shifts of tens of votes in both directions.

In 1978, a candidate for comptroller of the State of Illinois refused to believe he had lost Madison County by a large margin, and it turned out, according to Michael Hamblett, a member of the Chicago Board of Elections, that the totals had "flipped-here was a computer flip-flop."

That same year, in a statewide recount for secretary of state of Ohio (which Mark Braden, the present general counsel of the Republican National Committee, helped to conduct), only sixteen votes changed out of about three million. But overvoting on punch-card ballots was beginning to trouble Ohioans. Anthony Celebrezze, Ohio's secretary of state, estimating that about fifty-five thousand voters had had their votes invalidated in this way, asked, "Are they being partially disenfranchised by some peculiarity of the equipment itself"

In El Paso, Texas, the winner of a 1978 school-board race, Marvin Gamza, was deprived of his victory when the computer failed to count votes cast for him in three precincts, because ballot layouts from an earlier election had been used in them. Suspicions were voiced that the mistake had been deliberately left uncorrected, and the federal judge who heard the case, John H. Wood, was angered when he learned, from the television news one night, that some of the relevant ballots had been burned. He concluded that "a willful effort" had been involved in the error, rejected the claim of the putative winner, and installed Gamza on the school board. But Judge Wood was overruled on appeal, because Gamza had filed his protest too late. "The winner lost," said Malcolm McGregor, Gamza's lawyer, but McGregor doubted whether the mixing up of the layouts was premeditated, because, he said, "a baboon would not have tried to steal the election that way."

In 1980, computerized vote-counting faltered seriously in a number of jurisdictions across the country. A study by the city clerk of Detroit concluded that in a primary conducted on the C.E.S. punch-card system, which the city had just installed, votes on one out of every nine ballots cast had been invalidated-fifteen thousand in all because people had tried to vote in two parties' primaries.

In that same year, when a mark-sense system sold by Martel Systems, of Costa Mesa, California, was used for the first time in Orange County, California, a Republican stronghold, there was a four-day delay in the count. On Primary Night, more than fifty precinct-level memory cartridges had broken down, and-because of programming errors, it was explained-the computers had given about fifteen thousand Democratic-primary votes meant for delegates for Jimmy Carter or Edward Kennedy to delegates for Lyndon LaRouche and Jerry Brown.

Montana law permits voters to demand paper ballots, and in Missoula (where votes for Humphrey and Nixon had been interchanged in 1968) as many as thirty per cent of the voters chose to vote this old-fashioned way. Still in this same year,

-----|

1980, card readers broke down in jurisdictions in Michigan, Arkansas, Indiana, and Utah. In Salt Lake City, a central card reader started "putting out jumbled numbers on about three out of every hundred ballot choices," according to a news report. In a township in Ohio, two tax proposals were switched; the voters would have taxed themselves five times as much as they wanted to if the error hadn't been discovered after the voting. In Custer County, Nebraska, the county clerk said that a count on a C.E.S. system concerning a school-closing issue showed more people voting than were registered. The computer had also refused to read some ballots and had read only parts of others. In Bradenton, on the Florida Gulf Coast, a seventh of the county's precincts had to be counted twice, because "soggy, warped, and mangled ballots" occasionally jammed the computers. Directly across the panhandle, at Fort Pierce, on the Atlantic, new computerized machines counted Democratic ballots well enough but refused to accept Republican ones. "It was awfully strange," the supervisor of elections, James Brooks, was quoted as saying. "Those damn machines must have been built by the Democrats."

In San Antonio, Texas, in perhaps the most consequential breakdown in 1980, it was discovered that the C.E.S. program that counted votes in the Presidential election in Bexar County could not tally more than nine thousand votes for any race, so the computers had not counted many of the votes cast for Ronald Reagan and two other Republican candidates. The official post-election canvass found that sixteen-hundredths of a per cent fewer total votes were cast than had been reported on Election Night, whereupon the San Antonio Express noted, "As San Antonio moves into the computer age, the slogan of the universal suffrage movement becomes, 'One man, 0.9984 vote.'" The recount dragged on for several weeks, with local politicians pointing fingers at each other. Mike Greenberg, a columnist for the Express, learned that election officials had taken unmarked ballots home overnight. "Even already marked ballots could be tampered with," he went on to say, continuing, "Anybody with a straightened-out paper clip could punch out a few more holes to either spoil a ballot with the 'wrong' votes or cast 'right' votes in races ignored by the legitimate voter." In due course, Bexar County returned to lever machines.

A candidate for the school board in Carroll County, Maryland, in 1984, T. Edward Lippy, finished third, with about six thousand votes. When, in obedience to state law, the voted C.E.S.-system ballots were taken to an adjoining county to be recounted on a different computer system, about twelve thousand five hundred uncounted votes were found, and it was learned that in fact about nineteen thousand citizens had voted for Lippy. He was proclaimed the winner. The error was explained as a slip-up by a local data-processing official. ("It was my mistake," he said.) He had inadvertently replaced the correct C.E.S. provided program with a test program that would not count two votes if they were punched in one column on the ballot, and most of the voters who favored Lippy had also voted on a home-rule proposition in the same column with the numbered rectangle assigned to votes for Lippy. The wrong program had also cost President Reagan more than two thousand votes in the first count. A standard pre-election test had not caught the official's mistake; in a state without the requirement to double-check the count, it could have been missed.

In 1985, in Moline, Illinois, a candidate for alderman served for three months before a recount removed him from office. This mistake was laid to a slipping timing belt that had caused the card reader to fail to count a number of straight-party votes for the real winner. The apparently defeated candidate, it turned out, had actually won handily.

IN the fall of 1980, Michael Shamos, a computer scientist, law student, and businessman who was teaching at Carnegie-Mellon University, in Pittsburgh, and running a software company, saw an announcement on a computer bulletin board that the Commonwealth of Pennsylvania was looking for examiners for computerized-voting systems. He knew nothing about such systems, but the job sounded interesting, so he signed up and went to Harrisburg to examine the C.E.S. Votomatic system. "What I saw that day," he told me not long ago, "was hairraising and mind-boggling: antique, obsolete, unreliable technology packed with a systems approach that was even more unreliable."

We were talking in the upstairs study of Shamos's home in Pittsburgh. On the wall above his desk was a large Princeton University pennant. He has degrees in physics from Princeton and Vassar; an M.S. from American University in the technology of management; three degrees in computer science, including a doctorate, from Yale; and a law degree from Duquesne. Shamos continued, with feeling, concerning the Votomatic system, "Counting paper ballots is no picnic. I really thought hard about this. Am I being picky? I came to the conclusion that it's far worse than a paper ballot. After all, what is the rush? I for the life of me couldn't figure out why anybody would use this."

That November, Shamos presented to Pennsylvania's Bureau of Elections his evaluation of the C.E.S. election system. Punch-card technology was obsolete, his report stated. The C.E.S. system had not been modernized and was "a security nightmare, open to tampering in a multitude of ways," Shamos continued. "It is apparent that security was not taken seriously as an issue during the design of the Votomatic." The report went on to note that the ballot pages in the Votomatic booklet could easily be shuffled or replaced; blank punch-card ballots were easy to obtain; and the plastic seals on the boxes used to transport voted ballots for central counting were easily duplicated. Moreover, the system could not be verified

without examination of its source code, yet C.E.S. had refused to produce that code; no effort had been made to restrict access to the control panels or the toggle switches on the computer, with which "any person can enter arbitrary numbers into the machine's counters;" and the counting program, loaded through a deck of punched cards, could be altered to change the counting "by inserting or deleting a single one of the cards or by transposing two of them."

Shamos now warned, "The following scenario is thus fully possible. A would-be election fixer enters a voting booth with a card concealed on his person that, when read by the tabulating computer, will reset its counters to values desired by the fixer. On leaving the booth, he presents this card, conveniently wrapped in its secrecy envelope, to an election official who, not being permitted to examine it, drops the 'ballot' into a box. After the election, the card makes its way to the central counting facility where it is read by the computer. Instead of being counted as a vote or rejected by the system, the effect of this card is to change the current vote total for any candidate desired."

In a carefully worded paragraph headed "Concentration of Control at C.E.S.," Shamos noted, "All software used in the Votomatic machines is obtained in the form of secret card decks supplied by C.E.S. Without casting doubt on the integrity of C.E.S. in any way, nonetheless, the possibility exists that an unauthorized person may gain access to the central point from which these programs are distributed and alter them. The implications are frightening when it is remembered that one-quarter of all votes cast in the U.S. are counted by these programs."

Throughout the evaluation, Shamos wrote, C.E.S. "took the attitude that the Votomatic system has been in use for seventeen years, has been evaluated by more than thirty states, and has never been denied certification. In response to virtually every question regarding a deficiency, the vender responded by stating that the problem had been considered by a number of other jurisdictions and was found not to be serious.... The Votomatic system must be denied certification."

Pennsylvania assigns three examiners to inspect each voting system submitted for certification, but the decision about it is made not by them but by the secretary of the Commonwealth. One of the other examiners found the system acceptable. The third, C. Kamila Robertson, of the computer-science faculty at Carnegie-Mellon (who said that the voting booklet had come apart in her hands, and that "it would be easy to sabotage the computer in this system ... the switches are there for the switching"), agreed with Shamos. The secretary of the Commonwealth certified the system, but Shamos's report soon became one of the basic documents in the controversy over computerized vote-tallying.

THE precinct-level corruption that Joe Harris had witnessed in Chicago in the twenties was visible again in the 1982 election there, but now instead of repeat voters the precinct captains had repeat votes, as counted on the C.E.S. system. According to the report of a grand jury that investigated the 1982 election, and whose indictments led to fifty-eight convictions, ward committeemen appointed city employees as precinct captains, and these factotums either produced for the political machine on Election Day or lost favor with their patrons. The grand jurors reported, "One precinct captain and his son disregarded the actual ballots cast by voters and instead held their own fraudulent election after the polls closed by running two ballots through the voting machine. One ballot was a straight Democratic 'punch 10.' That ballot was counted by the machine a total of one hundred and ninety-eight times. To make the results less suspect, they also counted a ballot containing some Republican votes a total of six times. Consequently, all but two of the voters in that precinct were disenfranchised."

The grand jurors said that in many Chicago precincts in 1982 faked punch-card votes were cast in the names of transients, the ill, the incapacitated, and people who had moved away, had died, or had not voted. Runners worked the boarding houses and hotels to find out who was not coming to the polls. "The ballots either were punched on the voting machines by people posing as the voter, or were punched with ball-point pens or other similar objects in a private place outside the polling area," according to the grand jury's report. In one named precinct in the Thirty-ninth Ward, the captain gave lists of non-voters to one of the election judges, and she slipped them into her shoe. During the day, she would draw out a list when no one was looking and forge names from it on blank ballot applications. "The precinct captain and others apparently retreated to the privacy of the men's washroom to punch some of the ballots," the grand jurors said.

THE legal conflict that perhaps best embodies the doubts about computerized democracy, and demonstrates-whether the plaintiffs or the defendants were right in this particular case-many of the difficulties of proving charges of stealing elections by computer, started in Charleston, West Virginia, in 1980 and ended, for all practical purposes except for the plaintiffs' liabilities, in a federal appeals court in Richmond, Virginia, in 1986. In 1971, Jack Gerbel, of C.E.S., and an area C.E.S. representative had presented the Votomatic for approval in West Virginia, but the state's two examiners rejected it. They cited its permitting of overvoting, and they stated, "The computer program ... can possibly be modified by an experienced data-processing person, causing the computer to miscount votes cast for a particular race." However, the West Virginia secretary of state, Jay Rockefeller (who is now United States senator from West Virginia), seeing, as he wrote at the time,

-----|

that the report of the examiners was negative, designated two new examiners, and they approved the system.

At about 7 P.M. on November 4, 1980, as Ronald Reagan was being elected President, Walter J. Price III, a plump-cheeked, energetic young man in a blue blazer and khakis and his "Election Day" tie-blue with diagonal gold and red stripes-drove down to the voter registrar's office in Charleston. A freshman Republican legislator in a county that Daniel Boone had once represented in the Virginia Assembly, Price was going downtown to see himself reelected, as he thought, and to watch the operation of the new system the county had bought the year before from C.E.S. He was not worried about vote fraud, he told me later, because the first clerk of Kanawha County the Republicans had had since 1932, Margaret (Peggy) Miller, would be running the count.

Over the vehement objections of the voter registrar, Carolyn Critchfield, Price threaded his way among desks and people toward what the election workers called the computer cage. This was a small room with windows on all sides that began about four and a half feet above the floor and a Dutch door that had a window in its top half. The two vote-counting computers of the BT-76 (Ballot Tab) system in Charleston, one of them designated the "master" and one the "slave," had been set up on the floor inside, with punchcard readers on top of them and printers beside them. On the computers, down near the floor, were sets of toggle switches. Price has testified under oath, and repeated in greater detail during lengthy interviews with me, that, as he walked around the outside of this room looking in during the next hour and a half, he saw four kinds of actions, which, four and a half years later, dominated the only known court trial so far of charges that an election was stolen by computer. The people who Price said took these actions have all vigorously denied doing so, also under oath.

Traditionally on Election Night in Kanawha County, the vote totals were announced and posted in the precincts. This year, none were. Instead, the uncounted voted punch cards were all carried from the precincts to the registrar's office and run through one central system, which Walter Price was looking at. Only these cumulative centralized counts, which included no record of precinct-by-precinct totals, were coming out of the whining, clacking printers; then they were ripped loose and fed to the local reporters and to the citizens who had gathered on the other side of the chest-high reception counter.

Price said that at least four times while he was looking into the computer room that night he saw Peggy Miller, the county clerk, drop down into what he called a coal miner's squat-"not on her knees but bent down with her knees coming up toward her chest"-in front of the sixteen toggle switches on the master computer, consult notes she had on a pad or clipboard, put the notes down, turn a key, flip some of the switches, and turn the key again. Such an action was not called for in the counting of the votes. After Peggy Miller finished flipping the switches, Price said, she reclaimed her notes and stood up. On more than one of these occasions, she walked over to the nearby "dasher," a slow printer, "and she would type some things and then the printer would run," he said.

The incumbent congressman for that district, running again, was a Democrat, John Hutchinson. He had been elected the mayor of Charleston three times in the seventies, and in 1976, during his service at City Hall, he had run for governor, but had lost. Although he and Jay Rockefeller, who in 1980 was the Democratic governor, were not friendly, Hutchinson was regarded by Walter Price as one of the five most influential Democrats in the state. Mick Staten, Hutchinson's Republican opponent, was a close friend of Peggy Miller's husband, Steven, a lawyer, who was the general counsel for the Republican executive committee of that congressional district, and Staten's largest campaign contributor. Hutchinson had trounced Staten in a special election the preceding June, and two polls conducted by the Charleston Gazette had predicted that Hutchinson would win again, in the counting that Price was watching, by a spread of between fourteen and sixteen percentage points; that is, by around twenty-five thousand of the votes that were being counted. Hutchinson's wife, Berry, said that a poll by the Democratic National Committee, too, had shown that her husband would win by a wide margin. Staten himself, however, had predicted that he would win, by five points.

Price said that during the counting his fellow-Republican Steve Miller entered the computer cage, drew out of the inside pocket of his suit coat a pack of cards between a quarter of an inch and an inch thick and the same size as the ballot and control punch cards, patted the cards to even them up, and handed them to his wife. According to Price, they were talking, but, being behind the glass, he could not hear what they said. Price testified that Peggy Miller ran the cards through the card reader, retrieved them, and gave them back to her husband, and that he returned them to his breast pocket and left the room.

Seated at a table lodged between elements of the C.E.S. system was a man Price had never seen before. Clearly, the person he was referring to was Carl Clough, the Northeast sales manager of C.E.S., who had been with the company for ten years. Price said he saw this man busily using a telephone and what seemed to be a calculator. Open in front of him on the table was a large case resembling a briefcase. Three or four times, Price said, the man grasped the phone as one might

the handle of a suitcase, and, he told me, he "places it, he very carefully places it" in the case; he "pushed it down ... it was just a very deliberate pushing in" of the phone. After a time, he said, the man put both hands to the case, seemed to hold it down with one hand "like he was steadying, like there was some resistance to," the phone's "coming out," and, with the other, pulled the phone out "with some force." This resembles a description of a man using a modem, a device that permits computers separated by hundreds or thousands of miles to communicate with each other over telephone lines.

The operator of the master computer that night was Darlene Dotson; the secondary, slave computer was the responsibility of Vicky Lynn Young, just two years out of high school. Vicky Young needed to keep her job, because she was taking care of some of her close relatives. Nevertheless, later, on the witness stand, she swore that on one occasion during the counting in the cage Clough "told me to go over and stand beside Darlene and help her with her computer so that nobody could see."

Had this happened? Clough was asked during the trial. "Absolutely not," he replied. Furthermore, he said, he had had a briefcase in the computer cage, but there had been neither a modem nor any other electronic equipment in it. He thought that he had used a phone in the cage, but that it could have been moored in an adjacent room. Young testified that Clough had tools but had not used a modem; he denied that he had any tools. Dotson averred twice before the trial that there had been a phone in the room and that Clough had used it "more than once;" at the trial she said there had been a phone jack in the room, but no phone.

Peggy Miller said on the stand that she had not gone into the computer cage at all on Election Night, thereby denying Price's testimony. (Mrs. Miller, who has resumed her former career as a schoolteacher, and is a candidate for the state legislature on November 8th, later said to me of Price, "He lied in court," and she also said, "He'll testify against his mother if it'll get him something.") Steve Miller, asked by the lead attorney for the plaintiffs, John Mitchell, "Did you enter the computer room and take several computer-sized cards out of your pocket and lay them down?" answered, "Absolutely, positively no." Clough said the Millers had not been in there while he was, although he had "stepped out a few times." A county commissioner said that he had seen Peggy Miller in the room. Dotson said that the Millers were not there and that Peggy Miller "may have come in, but not all the time." Young "didn't remember" Peggy Miller there, and said that she did not see Steve Miller come in "that I remember."

In a document having to do with an appeal, the defendants described Price's testimony as uncorroborated and "soundly contradicted by every other witness called by plaintiffs who was in a position to observe the occurrences in the computer room." They characterized Young's testimony as a denial that Peggy Miller had manipulated the toggle switches; they stressed that Price had not known the identity of the man he had seen with the briefcase.

On the night in question, Price, following the returns, perceived that he was losing his position in the House of Delegates, and after saying so to a friend of his he exclaimed loudly, pointing to the computer cage, "The only election I lost was in that room!" Hutchinson, too, lost that night, and by nearly ten thousand votes-the five percentage points by which his opponent, Mick Staton, earlier that fall had predicted his own victory.

Leonard Underwood, a Baptist minister, who had been defeated for the legislature by seven votes, challenged the Charleston results in a lawsuit, but Peggy Miller said that sixty-two days after the election-just two beyond the earliest legal moment in the absence of a contested election-she had had the punch-card ballots destroyed, not realizing that Underwood's challenge was still pending. "Anytime an election is completed ... those materials are cleaned out," she said. "Otherwise we would have a continuous buildup of materials."

T. David Higgins, a Union Carbide computer specialist who was also the chairman of the Kanawha County Republican Party, testified during the trial that in Charleston in the summer of 1981, at a political affair for Representative Staton, he had spoken at length with Steve Miller:

He was very unhappy with the fact that I was working with the joint House-Senate subcommittee here at the Capitol which was looking into the whole question of electronic voting in the state of West Virginia. And he also said something to the effect of how it worked out that my working with them, collaborating with them, somehow in his mind cast aspersions of.... He suggested that I thought there was something irregular in the election of November, 1980, here specifically in Kanawha County.

I said to him at that point that I did not think they had done anything wrong in the election of 1980. I said to him, "I do not think that you understand enough about this computer to rig it to fix an election." And Steve looked me in the eye, grinned

like a shark ... and said to me, "You underrated us."

(In a recent interview, Steve Miller denied that he had said "You underrated us" to Higgins at the Staton affair. "He told me about reports he had heard from Democrats that 'you guys had stolen the election,' and that he had told them we weren't smart enough to do that," Miller said. "And he's right, I grinned like a shark. In fact, I laughed out loud. I told him, 'Thank God, neither are you, David,' and turned on my heel and walked off." Miller went on to describe Higgins as "a conceited, arrogant fop" and "a shallow idiot." On the subject of Walter Price's testimony, Miller said, "He's a liar. I've never been in that computer room in my life." As for Price himself, he said, "If I had a choice between sitting down with him and a polecat, I'd pick the polecat.")

C.E.S. officials in Berkeley, upon learning of the rising public alarm in Charleston, sent out one of their programming consultants, C. Stephen Carr, who had probably written or revised as many of the codes for votecounting machines as anyone else in America. Testifying at hearings on electronic voting that had been called by the West Virginia secretary of state, in Charleston, Carr declared, "While any computer system can be penetrated, the time and effort to penetrate this one is so extreme as to render it effectively impenetrable."

Representative Staton was defeated for reelection in 1982. The West Virginia legislature passed a law that year requiring that after each election "at least five per cent of the precincts shall be chosen at random and the ballot cards cast therein counted manually." A special grand jury that was convened to investigate the November, 1980, election indicted Peggy Miller on six felony and nine misdemeanor charges of election-law violations, none of them directly related to the computers, and she was tried and acquitted on all counts.

THREE of the Democrats who had lost in 1980-Hutchinson, Underwood, and Bill Reese, a candidate for county commissioner-continued to be troubled by the outcome even after Miller's acquittal. Underwood wanted the three of them to sue for damages.

John Hutchinson told him, "Why, you're crazy as a bedbug, they beat me by ten thousand votes."

Underwood replied, "If you're gonna steal it, you can put in ten thousand as easily as ten."

Dozens of times, driving past the Hutchinsons' home, which is near his own in Charleston, Walter Price recalled, he thought that he should go in and tell Hutchinson what he had seen in the computer cage. "It occurred to me that that poor man ought to know what really screwed him out of Congress," Price said to me. "Why I didn't do it I don't know."

In mid-1982, though, he said, he happened to take a seat in front of the Hutchinsons at a public meeting in the state capitol, and Berry Hutchinson, a shrewd and ebullient woman, who is a member of an old-money Charleston family, leaned forward and asked him, "Were you by any chance present when the ballots were being processed in 1980?"

"Well, yes, I was," he replied.

She told him she and her husband would buy him lunch in the basement cafeteria if he would tell them what he had seen.

"For about thirty-five seconds," Price told me, he flinched mentally at "having truck with Democrats" and at having everybody see him walk through the capitol with John Hutchinson, but then-"It was a flash of lightning"-this response was erased by the thought Well, hell, you've got to do what's right. Price thereupon said he would go. Over lunch, he said, he described to the Hutchinsons what he had seen, and during a visit to the computer cage after lunch he showed Berry Hutchinson the toggle switches on the front panel. Outside the registrar's office, she said later, she asked him whether he would testify if they filed a lawsuit, and he said yes.

Early the next year, John Hutchinson, Underwood, and Reese, their evidence dramatically fortified by Walter Price, sued the Millers, the registrar of voters, the county commissioners, C.E.S. and four of its employees, and others for about nine million dollars in damages, alleging (in their third amended complaint) that various of the defendants had "tampered, directly and/or indirectly, with the computer programming of the election computer" and "rigged the counting computers by the manipulation of control toggle switches and the use of predetermined material or both in such a way that the computer did not reflect an actual count of ballots cast." The plaintiffs contended that by these and other means they had been deprived of "their constitutional right to vote or receive votes [and] their right to hold public office," and of income, reputation, time, and money.

Needing a computer expert, the plaintiffs turned to Wayne G. Nunn, a slender, soft-spoken man of thirty-six who was a project scientist for Union Carbide, one of the major chemical companies in West Virginia's Chemical Valley. Nunn had supervised the design and installation of computer networks, some costing several million dollars, for the firm's laboratories and pilot plants. He had shared an office there for three years with David Higgins, who was the chief of Union Carbide's computerized technology-intelligence-information network. Nunn also ran a small custom-software venture that wrote programs, did consulting, and sold operating systems. He had programmed computers in many different computer languages and in the field of artificial intelligence.

Having no confessions from any of the defendants, John Mitchell determined to rely on circumstantial evidence in trying to prove a conspiracy. Three weeks before the 1984 Presidential election, Nunn conducted a nine hour examination of the C.E.S. system, with Carr, who had programmed it, Kemp, the C.E.S. president, and a dozen or so other people watching. Because of a clerical slip-up in the listing of what Nunn wanted to see, C.E.S. was not required to show him the source code, the diagrams for the circuit boards, and the operators' manuals. Nevertheless, feeling his way along in the microcosmic darkness of the program's space, Nunn, with one punch card, added ten thousand votes to the total of one of the candidates in a mock race for President.

During a deposition he gave subsequently, under extensive cross-examination by an attorney for the Millers, Nunn said that he had perceived seven ways in which the C.E.S. system in use in Charleston could be caused to miscount the votes: by manipulating the toggle switches on the face of the Data General Nova computer to change vote totals and the figure for total votes processed; by altering the program deck of cards during the counting; by running "summary cards" through the computer to add votes for candidates; by changing vote totals using the keyboard at the slow printer that was part of the system, using another computer located nearby and connected by a cable, or using a computer thousands of miles away, by means of modems; or by planting a "Trojan horse" (hacker jargon for secret, undetectable commands that can be hidden in a computer program) in the code that controls the vote-counting, requiring it to switch, say, one out of every four votes from one candidate to another or give a candidate a false victory by a certain percentage.

The plaintiffs were determined to make a second effort to break the source code, and C.E.S. was determined to prevent Nunn from studying it. C.E.S. asked Judge Charles H. Haden II, of the United States District Court, whose wife had been the chairperson of Reagan's reelection campaign in West Virginia, not to let Nunn even see the code, because it was "a 'trade secret' . . . highly confidential." Alternatively, the company said, if the Judge forced them to let Nunn inspect the code Nunn should have to do it at C.E.S. headquarters in Berkeley and should not be permitted to copy it or leave with any notes.

Hutchinson and his fellow-plaintiffs assailed the C.E.S. insistence on secrecy from a broad perspective. "There should be full disclosure of matters involving public elections," they contended. "[The] demand for 'secrecy' by C.E.S. only insures that the potential for fraud will be perpetrated. This involves a matter of strong public policy." (Perhaps the plaintiffs meant "perpetuated," but their motion said "perpetrated.")

Judge Haden ordered C.E.S. to make the source code available to Nunn in Charleston, but he ratified the company's practice and requirement of secrecy, and he decreed, "Dr. Nunn will not reveal any information to anyone.... No records shall be made of information obtained." (During the trial, the Judge stated from the bench, "They are entitled to protection of the secrets.") But the litigants had extracted their minimum requirement: Nunn had the code, and he examined it to his satisfaction in a closed office at the local C.E.S. attorneys' firm for parts of two days.

What he had was a printout of "the assembler third pass listing" for the BT-76 program—a stack of computer paper still joined together at the folds which was four or five inches high. He was allowed to make notes but was not provided with the computer he needed in order to test the code systematically; all he could do was look at the highly technical lines of the listing. This was grueling mental work, and after three or four hours he was very tired. During the second day, he decided there was nothing more he could learn from just looking, sealed his notes, gave them to the C.E.S. lawyers, and left.

Carr and Kemp flew to Charleston to crowd into the computer cage again and watch Nunn's second examination of the system. As the day wore on, the number of people watching varied between ten and twenty-five, and sometimes Nunn could hardly move around. Mustachioed, skinny, and dapper in a blue suit, he examined the inside of the computer with a long black flashlight, tested again how it worked, and printed out results of a mock election. He announced that with the toggle switches he had been able to manipulate the figure printed out on a cumulative report for total ballots counted.

Several hours later, after further examining the machine, Nunn cast and counted one punch-card ballot, with just one vote on it, printed a cumulative report that showed one cast and counted, stopped the computer, used the toggle switches to change the vote for Position No. 1, re-started the computer, printed out, and, showing the printout, announced, "The next

report is a cumulative report, again showing one precinct processed, one ballot processed. But Position No. 1 now has ten thousand and thirteen votes." Then, again with one ballot, he produced five votes. Then seven. "No punch cards were necessary," he told me later. "I could have produced the result of ten thousand or any number we wished without counting a single ballot."

THE 1985 Charleston trial was conducted between April 9th and May 2nd in a federal courtroom within a few blocks of the registrar's office, where the votes had been counted that November night in 1980.

Midway through the trial, Walter Price gave his account of what he had seen in the computer cage. After some gambits that Price parried easily, John F. Wood, Jr., the attorney for the Millers, pounced on two facts: that in handwritten notes Price had made on what he had seen he had not mentioned seeing Steve Miller give his wife the cards, and that in his deposition he had once called the cards "sheets of paper" and had not said that Steve Miller had taken them out of his coat pocket. Wood suggested to the jurors that the witness was making things up, and one of his closing questions was "That's your story today, isn't it, Mr. Price?"

"I would not characterize my testimony here as a story," Price retorted. While Nunn was on the stand, the defense lawyers raised at least a hundred objections, and Judge Haden sustained about half of them. Mitchell had planned to have Nunn repeat for the jury, on Charleston's C.E.S. system, his demonstration of how to steal an election, but the attorney abandoned that because of positions the Judge was taking on the admissibility of testimony. "There will be no evidence presented in this case of a Trojan horse," Haden informed the jurors. "None will appear." Nunn was prepared to testify that a "debugger" in the BT-76 program, while enabling a programmer to make repairs in the program, was also a Trojan horse; Haden excluded such testimony. Nor would the Judge let Nunn testify that when he had examined the system he had found discrepancies in the locations of memory addresses for the storage of information.

The fact that the C.E.S. system had been officially approved for use in West Virginia had a perverse effect during Nunn's testimony. Fifty-nine standards for computerized vote-counting had been proposed in 1975 by Roy Saltman, a specialist on the security of computer-tabulated elections, in the then definitive National Bureau of Standards study on the subject. Nunn had concluded that the C.E.S. system sold to Kanawha County in 1979 violated thirty-nine of these standards, but Haden refused to let him say so, on the ground that the state's approval of the system rendered the Bureau of Standards report "immaterial."

Nunn managed to tell the jurors (sometimes only to have Haden order them to disregard the information) that vote totals could be directly changed by means of the toggle switches on the computer's front panel without leaving a trace on an audit trail, and that summary cards, which in the C.E.S. systems are the same size as the punch-card ballots, could be used to add votes to candidates' running totals. Nunn also testified that he had concluded that the program had been changed during the counting.

To alter a candidate's votes with punch cards, Nunn told the jurors, one does not need to know the candidate's location in the computer's memory; all one needs is the number of the candidate's ballot position (a number that anyone voting in the election can know). With that and one punch card, Nunn testified, "you can set his vote total in the cumulative counters or in the precinct counters to zero," and then, with a second card, "you give him, you know, ten million votes if you want."

When the plaintiffs rested, the defendants asked Judge Haden to render a directed verdict for their side and send the jurors home. The legal situation was clear. Before entering a directed verdict in a conspiracy trial, as defense lawyers observed in statements to the Judge, he was obliged to give the plaintiffs "the benefit of every reasonable inference," to read their evidence "in a light more favorable to them" to give it "favored treatment."

"I find," Judge Haden ruled, "that the only evidence that the 1980 election was rigged is purely speculative in nature; it was mere suspicion; and it does not form the basis for the Court ... to infer that a conspiracy may be present.... The plaintiffs have never proven the existence of a conspiracy or these defendants' membership in a conspiracy." The ruling continued, "Consequently, all we have in this case are a series of unrelated acts that have been proven, most of which have a reasonable and an innocent appearance as easily as they would have a culpable appearance, none of which ... are attributable to more than one individual or to more than one entity.... And there are certain things that have been attributable to the defendants," but "the proof of individual overt acts, however compelling some few of them may appear to be to plaintiffs' counsel, does not suffice for the absence of proof of the conspiracy." Haden entered directed verdicts for the defendants and dismissed the jurors after their three weeks' service.

A year ago, judge Haden entered a finding that the plaintiffs would have to pay the legal costs of the defendants, including

C.E.S., which Mitchell estimated would total about six hundred thousand dollars. Just two of the C.E.S. lawyers had billed the election equipment company for twenty-seven hundred hours' work on the case about fifteen working months-and Haden re-billed this to the plaintiffs, on his judgment that, despite the fact that an earlier judge had ruled the case not frivolous, it was "meritless." According to John Mitchell, almost everything that the three plaintiffs own is tied up by liens pending Haden's entry of his final order on costs and the resolution of the three defeated candidates' certain appeal from it. [is this why no one sues!!!!]

"C.E.S. wasted a lot of money defending a case totally without merit," Stephen Carr, the chief programmer for C.E.S., declared during an interview I had with him. We spoke in his office at Information Processing Corporation, his company, which does engineering work on computer products and consults on computer programming, in Palo Alto, California. "Three politicians who couldn't believe that the electorate hadn't voted for them felt that they were surely gypped by the system. They got a local Ph.D. consultant who worked at Union Carbide. He was not dumb, but he had essentially, you know, taken money to be their expert witness, and they tried to show how the program could be manipulated. The case was so bad that after they presented their side the judge threw it out of court-the whole thing just died."

What was Carr's view of the ten thousand-odd votes that Nunn produced with one summary card during the first demonstration?

"With summary cards, you put in totals and multiple counts," Carr agreed. "But they also, at least in our design, would leave a very noticeable mark on the tape. Anyone who was at all knowledgeable couldn't miss it: a record left that these votes had come in from a special control card, not from ballots. So I wasn't impressed."

Carr laughed and smiled, then continued, "This is funny. Nunn also spent a bunch of time trying to show how you would work from the front panel of the Data General computer called the Nova. It was front-panel switches that computers of that era had. And if you know enough and the people will let you, in half an hour or maybe twenty minutes you might manipulate what's inside the computer and change things."

Walking me back to a room that was almost filled with computers, Carr went to a Data General Nova there and gave me a demonstration of how to raise a storage location for data-sometimes called a memory address-into the lights and change the figures stored in it. "But the chance of doing this unnoticed is just nil," he said. "And doing it in a way that doesn't cause the whole program to stop is terribly tricky. You can always argue the theory that there's some superhuman who's smart enough, but it's so hard to do that that somebody that good probably doesn't use his talent to mess around with one vote-counting machine. I mean, it's not citizens in West Virginia; it's, you know, somebody that's the Godfather! It just doesn't play in my mind that someone that was that up to speed would care about the race in West Virginia. And, you know, they had all kinds of theories that we out in California cared about that race. What we wanted was to run an honest election and get paid. Not even to run an election-to provide the equipment that the local people could run an election on. And I will say, as an outsider, I never saw in my contact with C.E.S. people any evidence of any kind of impropriety, or even caring. The people I saw at C.E.S. were interested in making honest money."

Turning to charges about Trojan horses, Carr said, "There have been some people who say that the way to phony up these programs is to make them count correctly when the counts are small"-as in a pre-election test with, say, a hundred ballots-"and then cause a fudge factor to come in when the counts are large; you then bring in your bias."

Carr granted that someone could "put a special thing in the code that when it saw some special pattern it did some special stuff."

How could that be detected?

"You could certainly find that by examining the source code," Carr replied. "It would take a while."

I asked Carr about audit trails. He mentioned, as an example, "a printer that leaves a hard-copy record of what things happened in time."

Could such a printer be turned off? "You could imagine someone cutting a wire-you can imagine anything. If the election officials and the clerks were used to running the computer and the printer stopped, you'd pick it up right away, because the printer makes a loud sound. And, of course, typically these Election Nights there are representatives, or monitors, from all parties watching."

-----|

I also asked Carr about the possibility of fixing national elections.

One reason it would be very difficult for a single programmer at a major election company to fix a national election, he said, is that although the central source code is general, local election officials have to prepare instruction cards dealing with each local election's different candidates and their different positions on the different local ballots, "so that in one precinct Party One may be the Democrats, but in another precinct Party Two may be the Democrats, and the program then follows instructions to put all the votes for Democrats together. So it would be very tricky to, in this general program- If you set out to help one party in one state, you might totally screw yourself in another, it's just that tricky for the programmer back at C.E.S."

In a close Presidential election that would be decided in a few large jurisdictions "it wouldn't be impossible," Carr added.

I then asked him how, hypothetically, he himself might go about such an undertaking.

In response, Carr adverted to his basic position: "I just don't know how you'd do it. I really don't. Because, even with the computer doing the counting, there are so many people involved. It would take a major conspiracy. You'd have to have a lot of people-twenty, thirty, a hundred people-on your side. It wouldn't be one man. It certainly wouldn't be anyone who did the program." Even if a corrupt official is running the counting in a big city, "he still has to depend on a lot of staff," Carr said. "It would take at least one person from each of the disciplines-programming, the management-to really get a start on it, and then there'd be tremendous risks you'd be found out. I don't think it's doable."

WHAT had Wayne Nunn actually seen when he looked at the C.E.S. source-code listing in the lawyers' offices? What were the "secrets" he had learned? Bound by Judge Haden's protective order, could he talk about them? On a Saturday night last December, I drove from Charleston to Nunn's home, a ranch-style house in the town of Poca, ten miles away. We talked in the den, where he had an Apple Macintosh Plus on his desk.

Could he say whether he had found a Trojan horse, or more than one? "The only thing that I'm restricted from doing is telling you exactly the code that's in the program," he said. "It had lots of fascinating little nooks and crannies hidden around in it that no one has ever let me talk about. There are at least a half-dozen places, maybe a few less, where you could lay in a Trojan horse in that source code-lay in routines to do whatever you wanted to in an election-because there's code in that system that shouldn't be there, is not being used, is worthless to the operation of the system. It can be replaced with anything you want it to be."

Had Nunn found a trapdoor; that is, a place in a program where one can break down its security system and emerge undetected deep inside the program?

"Yes. There is one."

And had he found "wait loops" in the program which conceivably could control outcomes, or "Christmas trees"-Nunn's term for surprise packages in a program?

"They're all there. There are wait loops there. There are routines that are not documented in the manual and, from every way I can determine, do not work."

As we talked, Nunn got up from the couch, where he had been sitting, walked to his desk, and sat down at the Macintosh. "You continue to ask questions," he said. "I want to look for something here. I've come up with an idea." After about ten minutes, during which he went on answering questions, he called me over to the keyboard and invited me to add on the computer any numbers that came into my head. I added eight and thirteen, then two multi-digit figures; the sums printed on the screen were correct. "Now," he said from the couch, to which he had returned, "add two and two." On the off-the-shelf program of this standard brand computer two and two added up to five. In ten minutes, before my eyes, Nunn had made a Trojan horse for me. He printed the five-step program out and gave it to me. I still have it:

10 input x

20 input y

30 if x = 2 then x = 3

|-----|

40 print "The sum of x + y is", x+y

50 go to 10

Line 30 is the Trojan horse inserted into the program that makes two and two five. "I've told it every time it sees the number two, replace it with a three," Nunn said.

I asked him if signs of these various ways to interfere with the C.E.S. system could be kept out of its audit trails.

"All of them can defeat the audit trail, some of them better than others," he replied, with some feeling. "Because, you see, built into that system is the ability to turn the audit trail off. Every one of them you can turn off."

What about the test decks that are run through the C.E.S. systems before and after elections?

"That is the biggest joke in the world," Nunn said. "Anyone who knows how to run the C.E.S. BT-76 system can be trained to steal an election on it in twenty minutes. A summary card, anybody can do." Of the switches he said, "As long as they are out there on the front of the machine and they're turned on, someone has the ability to stop the machine and fool with the panel switches.... You have no control over what's done to the memory of the machine.

"But it's even more serious than that. I write this program. I go through it. I'm absolutely sure that I know exactly what it's doing. I compile it and punch a deck of cards and hand it to you. We meet a couple of days later down here at the courthouse and you run what you say is my program. There is no way on earth that I can stand there and watch that computer run and swear in a court of law that that is my program running. Now, it may have the same input and output, but as far as swearing that it's my program, I can't. I can't even look at the punch deck. Now, there may be a few people in the world who can look at the punch deck for the executable image"-that is, the program deck in object code-"and read the punch cards and recognize the instructions, but I can't do it. Damn few could. From that point of view, there is no security."

That night, Nunn told me, step by step, how to steal an election with the toggle switches that stick out of the front of the Data General Nova computers in some C.E.S. systems. "Briefly, using the toggle switches, what you do is you halt the computer," he said. "You examine the memory address at which the computer's halted-you make a note of it. You go to the memory location that holds the counter of the candidate that you want. You load the memory address for the candidate you want to fix into it, and you say, 'Load address.' Then you load the number of votes to give him and then you say 'Deposit.' That's wiped out his real count and given him a fraudulent count right then. If you want to go someplace else and do it-some other memory location-you do as many as you want. You just do this until you're finished. Then you load the address where the computer stopped. O.K.? And then you hit the button for it to continue. The program continues on exactly the way it was. There's nothing in the computer that- The computer never knows it's been halted."

There is no printout on any audit tape, Nunn told me. If a time-and-date record was maintained and someone noticed that the clock was running late, that would be the only clue.

NO matter how deeply public officials may dedicate themselves to it, the task of tightening up the security on Election Night computers will remain a daunting one-and, if complete security is the standard, impossible. The computer scientist Roy Saltman, at the National Bureau of Standards, who is the leading authority in the federal government on the subject, stresses in his new report, "Accuracy, Integrity, and Security in Computerized Vote-Tallying," published in August, that no manipulation of election computer programs has been proved, but he also warns of "the possibilities that unknown persons may perpetrate undiscoverable frauds," by, for example, altering the computer program or the control punch cards that manipulate it, planting a time bomb, manually removing an honest counting program and replacing it with a fraudulent one, counting faked ballots, altering the vote recorder that the voter uses at the polls, or changing either the logic that controls precinct-located vote-counting devices or the voting summaries in these units' removable data-storage units. The problem in this segment of the computer business, as in the field at large, is not only invisibility but also information as electricity. Secret instructions can be so well hidden in software, especially if the language is the lower-level assembly, that testers cannot be sure of finding them. Testing all the possible paths that a computer program (and therefore a hidden code) could follow through a punchcard ballot apparently could not be done comprehensively short of assigning the job to a second computer, and even then one runs up against what Robert Naegele has called "the polynomial problem"-the vastness of the programming possibilities in the inner space of a program. Mathematicians at Natre Dame, working with Deloris Davisson, a computer specialist, have calculated that the number of possible programming pathways for a program executed through a standard punchcard ballot would be two to the nine-hundred-and-sixtieth power-a one followed by two hundred and eightyeight zeros. "It's a number that my computer can't hold," Davisson said. At the merely mechanical level, computer

experts in a large jurisdiction cannot test punch-card systems for every voting possibility. "It's an infinity as far as our work is concerned," said Rick Fulle, assistant director of voting systems and standards for the Illinois Board of Elections. "For our purposes, it just can't be done." When a state examination of the C.E.S. system in Chicago was suddenly scheduled, Fulle said, the chairman of the state board demanded that all possible ballotpunch configurations be tested, but Fulle figured out arithmetically that running through the sixty-seven million-odd test ballots necessary would occupy twenty staff members full time for four hundred and seventy-seven years.

IF one regarded the manifold issues of computerized democracy in a reductionist way, perhaps the principal concern would be whether, in a close election, the Presidency can be stolen by means of computer vote fraud in several major jurisdictions.

Carr offered reassurance that although theoretically such a calamity could occur, it would be extremely difficult technically and would require too many confederates to be feasible.

Michael Shamos, the voting-systems examiner for Pennsylvania, does not believe that a large number of people would have to be involved. "This is false," Shamos replied when I asked. "One. One person. The point is that, the way things are going, a national mechanism exists that could be manipulated by anybody, from a single individual to a nationwide conspiracy. It's not whether it exists or not, it's the fact that the mechanism is there to make it easy."

The leading candidates for the Presidency are seldom separated by more than ten points, so "here's what we do," Shamos said. "Working in a company headquarters, I'm writing some election software, which will be sent by Federal Express to jurisdictions in executable object code. I'm going to program this thing so that if there are more than eight hundred people voting in a precinct I'm simply going to trade some votes, take them from other parties and dump them into the party that I want to win. So all the totals are going to be exactly right. I'm going to change ten per cent of the votes, or five per cent—some small number. And that software is going out to pivotal jurisdictions in the country. And that is going to shift the national election. It's easy for a programmer. And his superiors will never find it. There's no way to find it unless they do an exhaustive code audit themselves. And this is a solo effort—one guy who happens to be well placed. Of course, many others are involved, but they don't know."

If some jurisdiction that had been tested for more than eight hundred votes discovered that the program didn't count correctly, and returned it to the factory, the programmer would simply say there had been a glitch on the tape, or a bad ROM—a unit embodying "read-only memory"—"or some other technical mumbo-jumbo," Shamos went on. "And we have an election, and the wrong guy gets elected." If recounts discovered errors in some localities they, too, would be attributed to programming errors, he said.

Shamos believes it "not unlikely for some guy to realize one day, he's sitting there in the room in the midst of all those coding forms—he says, 'My God! I can control this whole thing!' " After all, Shamos said, "we have enough tales of hackers who when they found they could do something went and did it, maybe even not with malicious intent, just to show that they could do it."

He then pointed out a second possibility: "Of course, you can imagine that the venders of the system are in with certain politicians. The politicians agree, 'Yes, I'll buy this system, if you fix the election my way next time,' and they actually give orders to their subordinates to do it. That's always seemed somewhat less likely to me, because of the possibility of a whistle-blower. Then, the third possibility is tampering by someone not in the employ of the company, by a break-in at the vending company."

Summing up, Shamos said, "What does it mean that one company is controlling a large fraction of the voting in the United States? If you provide the software, you are controlling, even if you are not manipulating. Computerized vote-counting doesn't occur in the light of day, it occurs inside silicon in a little black box. That box is completely under the control of the vender, and if anything wrong happens we might never find out."

During an interview in a hotel lounge in San Francisco, Roy Saltman said, "If I broke into B.R.C.'s master computer program and changed the code, how about the nine hundred and ninety-nine other versions that are already out there? It's not a massive, central thing—all the computers are not connected to B.R.C. or to any single vender. There isn't any kind of central control that controls everything. I don't think that's a reasonable supposition. If you do the recount of the ballots, the whole thing falls apart."

Robert Naegele believes that no one person could steal an election by computer and, like Saltman, he does not regard

computerized theft of a national election as at all plausible. In a large jurisdiction like Los Angeles County, Naegele told me, five or six people would have to be involved, and hardly any jurisdiction is so centralized that one person could do it there. "My private opinion," he said, "is that there has never been any successful fraud in a computerized election. As I understand it, it's really not feasible. To do this, you require a hell of a lot of very sophisticated code.... I am not concerned about fraud on the national level. I don't think that's happened, and I don't think it's going to happen."

Like Carr, Peter Vogel, a computer lawyer in Dallas who was recently appointed an examiner of computerized voting systems by the Texas secretary of state, is skeptical that any conspiracy among large numbers of people would work, but, like Shamos, he thinks that the Presidency can be stolen by computer-"because of the electoral college."

Vogel said to me in his office, "If you have a majority in the right states, it doesn't matter who has the majority of the votes in the country. If you program the right states for the right elections, I think you could control the Presidential results."

Howard Strauss, of Princeton, gave me written answers to a series of questions about the possible rigging of United States elections by tampering with computer-tabulated election systems. He said that "there are many, many ways to do this," but all of them "can be largely eliminated" by rigorously followed procedures.

"If one software vender dominates the electronic-election market, subverting that vender may be the easiest way to alter national elections," he wrote. One individual, working alone, would be able to effect changes in the code more quickly and securely than a group, he believes.

What categories of people might fix computers in elections? I asked. Strauss replied, "In order of ease of subversion, some of the most likely groups or individuals include election-system vendors and their programmers and consultants, election-system operators, the Federal Election Commission, technical mavens of all kinds, and election officials and workers. It is possible that foreign agents, candidates and their staffs, and voters with special interests could subvert any of the above individuals or have sufficient expertise to subvert the process themselves."

Peter Neumann, of S.R.L, declared, "If somebody is a skilled user of a conventional computer system, he has the ability to do almost anything he wants and leave no trace, because most of the computer systems today do not have adequate protection or auditing facilities. Personal computers are non-secure, for the most part. Now, in the election systems the vulnerabilities are enormous. You effectively have to trust the entire staff of the corporation that is producing your software. Every single member has to be trusted. It would take one person to rig the system, typically, because of the way the thing is set up. There are very few internal controls."

Speaking in his office at S.R.L, amid papers stacked and scattered about on his desk and the floor and a chair nearby, Neumann went on, "Even if you can look at the source code, you can't guarantee that there's not a Trojan horse embedded somewhere in the code. Any self-respecting system programmer can hack the innards of the system to defeat encryption techniques or any password protection, or anything like that. All this stuff is trivial to break, for the most part. In most computer systems out there, it is child's play. Given the fact that the underlying systems are so penetrable, it is relatively easy to fudge data-for example, to start out with three thousand votes for one guy and zero for the other before the counting even starts, even though the counter shows zero. Essentially a Trojan horse in the coding. I can do it in the operating system. I can do it in the application program. Or I can do it in the compiler. I can rig it so that all test decks work perfectly well. I program it so that, after the test is run, at, say, six-fifty-five in the evening, it simply adds thousands of votes. It would never show up." He added that having a computer count a set portion of one candidate's votes as if they had been cast for his or her opponent would be "utterly trivial to do."

As for stealing a Presidential election, Neumann said, "I would put in a whole variety of techniques. I wouldn't just rely on one. You might use a different technique in each state, for example. You could trigger it so that you didn't do anything wrong if everything was going well, and if your candidate was losing you simply add votes-and you have to subtract, too. You have to make all the consistency checks satisfy. That's relatively easy to do."

Neumann exclaimed, "The possibilities are endless!" He seemed to be enjoying them, but then drew back. "I think the possibilities for rigging elections with computers are enormous. I'm not going to say it's ever been done. The point here is it's in the hands of one very skilled programmer or somebody who understands the system."

IN the face of such contradictory expert testimony, it is all but impossible for laymen to ascertain the precise degree of risk entailed by the use of computerized voting machines. Nevertheless, given the crucial role of public confidence in the integrity of the ballot, common sense suggests that the question should be resolved definitively, by the press and, perhaps,

by Congress. The press has begun to grapple with the issue, thanks in part to a series of articles by David Burnham in the Times a few years ago, and press coverage of contested computerized election contests has contributed to several reform efforts in the field.

With lever machines, the risk of vote-stealing has always been relatively easy to reduce. In one of the rules that Joseph Harris laid down in a model election-administration system, published by the National Municipal League in 1930, no lever voting machine could be used until it had been examined by "a competent mechanic." It is also necessary in lever-machine precincts that on Election Day candidates and representatives of parties be present at least twice-when the voting starts, to make sure that the counters are set at zero, and after the polls close, when the backs of the machines are opened, to read the totals. These are the moments of maximum opportunity for a vote-stealer: if he is not observed, he can simply turn the counters to obtain a desired result.

In the opinion of many specialists, there is only one comparably simple and effective way to deter fraud on Election Day in most computerized jurisdictions: an immediate hand recount of the ballots cast in a random group of precincts selected after the vote-counting by various parties to the election. Such a recount would be the greatest fear of anyone implicated in stealing an election.

When Harris reflected on the fact that computerized punch-card elections could be manipulated, he advocated, as a remedy, that every county and city using the Votomatic "set aside a number of precincts to count by hand and to compare the results from a hand count to the machine count." Who chooses the precincts? And when- before or after the election- does anyone know which ones they will be? Harris, in his model system, provided that "the candidates should be permitted to designate the precincts which they wish to have recounted and to amend and add to the list from time to time." "A manual recount of at least one per cent of the ballots of each contest is recommended," Roy Saltman wrote in his new report, and he added, "Responsibility for selection of some of the precincts to be recounted should be granted to candidates or parties." Michael Harty, now the Maricopa County elections director, in Phoenix, and the computer scientist Frederick Weingarten, of the congressional Office of Technology Assessment, suggest that voters who doubt the integrity of a computerized tabulation should, one way or another, at once secure the tabulating software as primary evidence.

Saltman also offered a set of recommendations that are not so easily carried out: all vote-tallying software should be obtained from an accountable source of stock offered publicly by reputable venders and should be scrutinized for "hidden code;" access to all stages of vote-tallying should be controlled; the ballots themselves should be carefully monitored administratively; every vote not cast by a voter in a race should be registered by voting machines as not cast; the use of pre-perforated punch cards should be ended, and perforations should be made unnecessary by the use of spring-loaded styluses. (The last change would require modification of the Voto-matics.) More broadly, Saltman recommended that the professional science of internal controls which is used in business be adopted in vote-counting.

Naegele proposed to the F.E.C. that vote-counting codes should be written in higher-level computer languages, because they are "quite a bit easier" to analyze for error or, for that matter, fraud. He told me, in California, that "the venders objected to this strongly," saying the vote-counting goes much faster in assembly (lower-level) language. A recent draft of the F.E.C. standards would make the use of high level languages "discretionary only." "What I wish," Naegele said, "is that some state would adopt a requirement for higher-level language, so the others would follow."

Ken Hazlett, the programmer who pioneered in the business with assembly language, expressed to me in Corvallis an opinion even more emphatic than Naegele's about the use of assembly language for computerized vote-counting: "Insane! It should all be in high level language, so there's a chance it'll be readable code twenty years later. There's no room for assembly except in some small isolated process."

The concepts of putting source codes in escrow and providing for their examination by independent test agencies seemed well established in the recent F.E.C. draft. Michael Shamos argued during my interview with him that escrow is not a workable concept for protecting election software (among other things, he wanted to know to whom private custodians of the code would be accountable), but the proposal is popular.

A number of other remedies, in addition to those in the studies by Saltman and the F.E.C's Clearinghouse, have been suggested by individuals in the election community.

Terry Elkins, whose inquiries and accusations concerning the 1985 mayoral race in Dallas led to the enactment of reform legislation in Texas, maintains that election officials should be made more accountable at law for their performances. Michael Harty, who suggested that programmers of election computers should be licensed, emphasizes the little-known fact

that most state election laws are not mandatory but "directory," and levy few or no penalties against officials who do not obey them. Paul Goldy, the president of the International Technology Group, of Woodbury, New Jersey, a smaller firm in the computerized election market, advocates user groups for local election officials, organized around specific products, like the groups that many computer buffs belong to. Shamos has proposed that persons who have criminal records for acts of "moral turpitude" should be barred from the vote-counting-equipment business.

R. J. Boram, the chief programmer of the R. F. Shoup Company, and Shamos advocate a high-prestige national election commission to test and certify vote-counting systems, including the software for them; Howard Strauss and a Princeton colleague have prepared for Election Watch, a small group that is working for change in this area, a specific proposal for a national testing authority. At a conference in Dallas sponsored by Election Watch, Strauss said that representatives of the vendors and anyone else who could change the counting program should be barred from computer rooms on Election Night.

Some citizens believe that vote counting software should be in the public domain, available to all parties and candidates, for whatever checks they wish to make on it. "I'm not for a public process being handled by private companies that won't let us see what's going on," says Susan Kesim, a young executive of a computer-security firm in Indiana. "Public-domain software -it's open. I want to see that it added one to the total, because that's the process of voting."

"Maybe a private foundation should do it," Frederick Weingarten has suggested. "Maybe if there was a consensus among the states, the federal government could write its own software and certify it through the National Bureau of Standards or the F.E.C. say, 'This we guarantee is accurate and untamperable.' "

Penelope Bonsall, the director of the F.E.C. Clearinghouse, said of the public-software concept, "It's a public policy question; it's too broad for us to consider. It would have to compete with private interests. I don't know who would fund it. I just don't see how you would eliminate private efforts in this area."

By 1984, the year before Joseph Harris, the exemplar of the entrepreneurial approach to computerized vote-counting, died, a subtle change had come over him. By then, lawsuits and accusations were bedeviling his baby, Computer Election Services, Inc. In a newspaper interview, Harris predicted that Americans would probably vote on TV monitors in voting booths, and computers would announce the winners minutes after the polls closed. But then he struck a note new for him, adding that these changes would not come for about twenty years, because such completely computerized voting would require "extremely careful management and planning to prevent error and fraud."

The new direct-recording electronic (D.R.E.) vote-counting machines, which New York City is preparing to buy on behalf of its three million registered voters, may become the realization of Harris's vision of futuristic electronic voting. When citizens vote on one of the D.R.E. systems, they address themselves to a printed ballot affixed to the face of the machine or displayed on a TV-like console and, with a finger or an electronic pointer, press on a box with an "X" in it beside their choice. The four surviving bidders in New York City are Cronus, Shoup, Sequoia Pacific, and, the one firm offering a TV-like system, the Nixdorf Computer Corporation, which is a wholly owned subsidiary of Nixdorf Computer, A.G., of West Germany. The bidders had to provide the technological capability to retain a record of "randomized" (that is, outof-sequence) electronic images of each voter's set of choices, but the city reserved the right to buy this capability or not.

Saltman's recent report indicated that the D.R.E. systems have one characteristic that from a security point of view may be even more important than the unavailability of real recounts if a voter's choices are not retained electronically. Since those choices are converted onto the counters inside the machines, there is no way to check from the outside whether they are recorded correctly. If the machine retained voters' choices on magnetic tape, the tapes would not necessarily be correct. Saltman wrote, "The fact that the voter can see his or her choices on a display, or even receives a printout of the choices made, does not prove that those were the choices actually recorded in the machine."

"There is no security in using a computer to count ballots," Wayne Nunn told me the evening he made me a Trojan horse. "I don't believe that computers should be used to count votes. I believe that what you should use for counting votes is a system that any voter can appreciate-in which he can fully understand all steps of the process. There shouldn't be any magic involved, because a computer system to the general populace appears to be magic. You put something in one end and, voila -something else comes out the other. A computer is such a flexible thing that what happens between the time when you put it in and the time when it comes out can be what any clever individual wants."

-RONNIE DUGGER