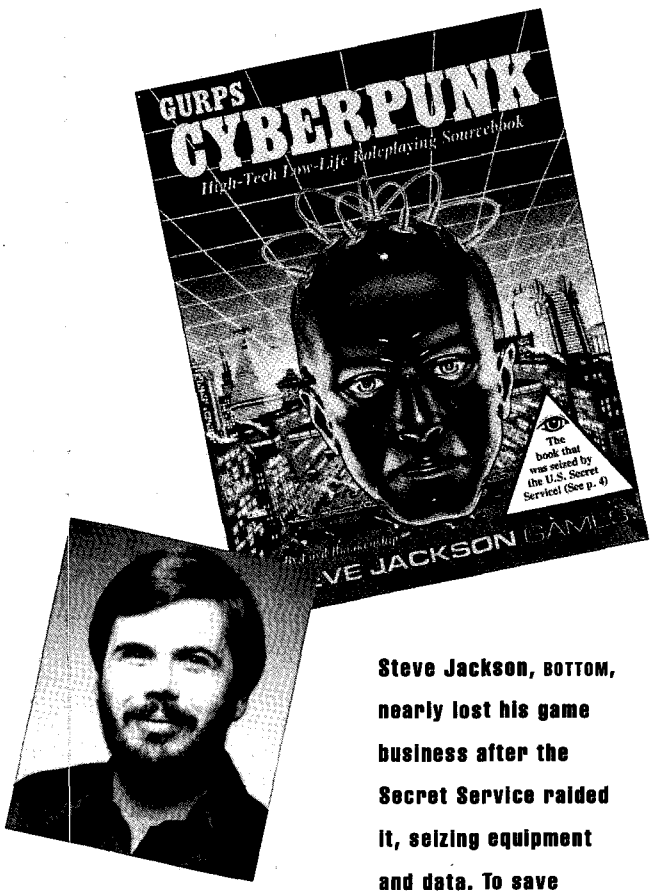
CLOSING



Steve Jackson, BOTTOM, nearly lost his game business after the Secret Service raided it, seizing equipment and data. To save the company, he and his employees had to reconstruct their new game, TOP, from memory.

Back in early February, newspapers

across the country reported that computer hackers were interfering with emergency calls over the 911 communications network. The reports said the hackers had penetrated the system using information from a secret computer document.

The scare grew out of an indictment by a grand jury in Lockport, Illinois. On February 7, Craig Neidorf and Robert Riggs were indicted on seven counts of wire fraud, violation of the Computer Fraud and Abuse Act of 1986, and interstate transportation of stolen goods.

Prosecutors alleged that Neidorf and Riggs had conspired to steal, using fraudulent methods, a confidential and proprietary document from the Bell South telephone company. This document, it was claimed, could allow computer hackers to disrupt the 911 emergency network.

The arrest of Neidorf and Riggs was only the beginning. The Secret Service, which has authority over crimes involving government computers, had embarked on a vast, nationwide investigation of hacker activity: Operation Sun Devil.

Imagine the night face of North America,

shining not with cities but with lines of light showing the transmission of data. Brightest are New York City, the financial capital, and California, the technological capital, with Washington, D.C., a close third. The lines that crisscross the country are telephone wires and cables, microwave transmissions, and packet-switching networks designed for computer communication. Here and there, beams dart into space to reflect off satellites and back to earth.

The computer networks in this country are huge. The largest are entities like UseNet and InterNet, which link every academic computing center of any size and are accessible to every scientist, university student, and faculty member in the nation. The networks also include government-operated systems, such as MilNet, which links military computers that do not carry confidential information. And there are the commercial services, such as Dow Jones News/Retrieval, SportsNet, CompuServe, GEnie, and Prodigy. CompuServe is the largest of these, with half a million subscribers.

In addition to these massive entities are thousands of tiny bulletin board services, or BBSes. Anyone with a computer and a modem can start a BBS; others can then call it up and use it. BBSes offer, in miniature, essentially the same services that the commercial nets offer: the ability to chat with others by posting messages to an electronic bulletin board and the ability to upload and download software and text files. There are more than 5,000 BBSes in the United States, most of them operated

THE NET

Will overzealous investigations of computer crime render freedom of the press technologically obsolete?

BY GREG COSTIKYAN

for fun. Few charge their users. In my local calling area alone, I know of BBSes for writers, gamers, Macintosh enthusiasts, gays, and the disabled—and I'm sure there are others.

The vast majority of BBSes deal with unexceptionable topics. But some boards deal with questions of computer security. These attract hackers.

Naturally, hackers discuss their hobby: breaking into computers. Usually, however, bulletin board discussions are general in nature. Hackers are not stupid, and they know that posting credit card numbers or the like is evidence of criminal activity. By and large, BBS discussions rarely, if ever, contain information that would be illegal if published in print form. It's not illegal, after all, to tell your readers how to commit illegal acts. If it were, books like *The Anarchist's Cookbook* and *Scarne on Cards* (and half the murder mysteries in print) would be banned.

The laws dealing with electronic transmissions, however, are far from clear. And the methods used to enforce these vague laws set a dangerous precedent for abridging freedom of speech.

In the future, the Net—the combination of all the computer networks—will be the primary means of information transmission, with print publication merely its adjunct. The Net will replace the press, and users of the Net must enjoy precisely the freedoms enjoyed by the press. If users of the Net have to worry about police surveillance, if censorship is rife, if the state forbids mere discussion of certain topics—then the liberty for which the Founders fought will have been destroyed, not by war or tyranny, but by mere technological change.

From the government's point of view, the arrest of Neidorf and Riggs did not end the threat to the 911 network. The document they had stolen was not a single piece of paper that could be returned to its rightful owner. It was an electronic document that Riggs had downloaded from a Bell South computer.

Riggs belonged to a hacker group called the Legion of Doom, whose members shared information. It was likely that others in the group had copies of the 911 document. Worse, Riggs had uploaded the 911 document to a bulletin board service in Lockport, Illinois. Neidorf had downloaded the file from the Lockport BBS. Anyone else who used the same BBS could have downloaded it, too, meaning that dozens of people might have this dangerous information. Worse yet, Neidorf had published an edited version of the Bell South document in an issue of his underground computer magazine, *Phrack*.

Unlike conventional magazines, *Phrack* never saw a printing press; it was distributed electronically. After preparing an issue, Neidorf would dispatch it, via various computer networks, to his address list of 1,300 names. Any recipient could then upload the magazine to a bulletin board or to one of the academic or commercial nets. That meant thousands, perhaps millions, of people had access to the information in the Bell South document.

We may imagine that the Secret Service was gravely concerned about the potential threat to emergency services. If not, their subsequent actions are hard to fathom.

On March 1, 1990, employees of Steve Jackson Games, a small game company in Austin, Texas, arrived at their place of business to find that they were barred from the premises. The Secret Service had a warrant, and the agents conducting the search wouldn't let anyone in until they were done.

The agents ransacked the company's offices, broke a few locks, and damaged some filing cabinets. They searched the warehouse so thoroughly, says company founder Steve Jackson, that afterward it "looked like a snowstorm," with papers strewn randomly. The agents confiscated three computers, a laser printer, several pieces of electronic equipment (including some broken equipment from a storeroom), several hard drives, and many floppy disks. They told Jackson they were seizing the equipment "as evidence" in connection with a national investigation.

Among the equipment seized was the computer through which S.J. Games ran a BBS to communicate with customers and freelancers. It had never been a congregating point for hackers and was about as much a threat to the public order as a Nintendo game.

The loss of the equipment was bad enough. Worse, the Secret Service seized all existing copies—on hard drives, floppy disks, *and* paper—of S.J. Games' next product, a game supplement called GURPS Cyberpunk. The loss of that data shot Jackson's publication schedule to hell. Like many small pub-

lishers, S.J. Games runs on tight cash flow. No new products, no income. No income, no way to pay the bills.

Over the next several weeks, Jackson was forced to lay off about half of his 17 employees. By dint of hard work, he and his staff managed to reproduce the data they'd lost, mostly from memory. S.J. Games finally published GURPS Cyberpunk as "The Book Seized by the Secret Service." It has sold well by the (low) standards of the field.

Jackson estimates the raid has cost him more than $125,000, a sum a small company like his can ill afford. (The company's annual revenue is less than $2 million.) He was nearly put out of business by the Secret Service.

What justified the raid and the seizures? Apparently, this: The managing editor of Steve Jackson Games is Loyd Blankenship. Blankenship ran The Phoenix Project, a BBS of his own in the Austin area. Blankenship consorted with hackers. He was fascinated by the computer underground and planned to write a book about it. He may or may not have once been a hacker himself. He certainly knew and corresponded electronically with admitted members of the Legion of Doom.

It turned out that the 911 document, which had given rise to the whole investigation, was neither secret, nor valuable, nor dangerous.

But perhaps Blankenship's worst luck was this: An issue of Neidorf's *Phrack* magazine included an article titled "The Phoenix Project." As it happens, that article had nothing to do with Blankenship's BBS of the same name. But the Secret Service was well aware of the contents of *Phrack*. Indeed, the revised indictment of Neidorf and Riggs, issued in July, cited the article by title. The same morning that the Secret Service raided Steve Jackson Games, agents awakened Blankenship and held him at gunpoint as they searched his house. They seized his computer and laser printer as "evidence."

Consider the chain of logic here. Robert Riggs is accused of a crime. Riggs belongs to a group. Loyd Blankenship is friends with other members of the group, though not with Riggs himself. Steve Jackson Games employs Blankenship. Therefore, the Secret Service does grievous financial injury to Steve Jackson Games. This is guilt by association taken to an extreme.

Neither Blankenship, nor Steve Jackson Games, nor any company employee, has ever been charged with so much as spitting in a public place. The Secret Service refuses to comment, saying only that S.J. Games was not a target of the investigation.

The company is now receiving legal help from the Electronic Frontier Foundation, an organization devoted to promoting civil liberties in electronic media. The Secret Service has returned most—but not all—of the company's seized equipment. Some of it is broken and irreparable. The government has made no offer of restitution or replacement.

On May 8, 1990, the Secret Service executed 28 or more search warrants in at least 14 cities across the country. The raids involved more than 150 agents, plus state and local law enforcement personnel.

According to a press release from the U.S. Attorney's office in Phoenix, the operation targeted "computer hackers who were alleged to have trafficked in and abused stolen credit card numbers [and] unauthorized long-distance dialing codes, and who conduct unauthorized access and damage to computers." The agency claimed the losses might amount to millions of dollars. In later releases and news reports, that figure was inflated to tens of millions of dollars.

Nationwide, the government seized at least 40 computers and 23,000 disks of computer information. In most cases, the subjects of these searches have remained anonymous. Presumably, they have either been advised by counsel to remain silent or have been so intimidated that they wish to attract no further attention.

John Perry Barlow reports in *Whole Earth Review* that the Secret Service held families at gunpoint while agents charged into the bedrooms of teenage hacker suspects. He adds that some equipment seizures deprived self-employed mothers of their means of support. These reports remain unconfirmed. It's clear, however, that the Secret Service closed down a number of BBSes by the simple expedient of seizing "as evidence" the computers on which those BBSes operated.

Bulletin board services are venues for speech. They are used mainly to exchange information and ideas. Nothing in the nature of the technology prevents the exchange of illegal ideas. But in a free society, the presumption must be that, in absence of proof to the contrary, the use of a medium is legitimate. The Secret Service has not indicted, let alone convicted, the operators of any of the BBSes closed down on May 8.

If law enforcement officials suspect that a magazine, newspaper, or book publisher may be transmitting illegal information, they get a warrant to search its files and perhaps a restraining order to prevent publication. They don't, however, seize its printing presses to prevent it from operating. A clearer violation of freedom of the press could hardly be imagined. Yet that is precisely what the Secret Service has done to these BBSes.

One of the BBSes closed down was the JolNet BBS in Lockport, Illinois, which Neidorf and Riggs had used to exchange the 911 document. Ironically, JolNet's owner, Richard Andrews, had triggered the investigation by noticing the document, deciding it was suspicious, and notifying the authorities. He had cooperated fully with the investigators, and they rewarded him by seizing his equipment.

The Ripco BBS in Chicago was among those raided by the Secret Service. Operated by Bruce Esquibel under the handle of "Dr. Ripco," it was a freewheeling, wide-ranging board, one of the best known BBSes in the Chicago area. Speech was extraordinarily free on the Ripco board.

"I felt that any specific information that could lead to direct fraud was not welcome and would be removed, and persons who repeated violating this themselves would be removed from the system also," Esquibel writes. But just about anything else was open for discussion. Hackers did indeed discuss ways of breaking into computers. And the Ripco board contained extensive text files, available for downloading, on a variety of subjects to which some might take exception. For instance, there was a series of articles on bomb construction—material publicly available from books such as *The Anarchist's Cookbook*.

Along with the computer on which Ripco operated, the Secret Service seized two other computers, a laser printer, and a 940-megabyte WORM drive, an expensive piece of equipment. The additional seizures mystify Esquibel. "My guess is that after examining the rat's nest of wires around the three computers, they figured anything plugged into the power strip must have been tied in with [the rest] in some way," he says.

The Secret Service has yet to return any of Esquibel's equipment. He has yet to be charged with any crime, other than failure to register a firearm. (He had three unlicensed guns at his office; he informed the Secret Service agents of this before they began their search.) Says Esquibel, "The government came in, took my personal property to determine if there was any wrongdoing somewhere. It seems like a case of being guilty until proven innocent....It's just not right....I am not a hacker; [I don't] have anything to do with credit cards or manufactured explosives. Until the weapons charge I never had been arrested, and even my driving record has been clean since 1978."

It appears that the Secret Service has already achieved its goal. The Ripco board was a place where "dangerous" speech took place, and the agency closed it down. Why bother charging Esquibel with a crime? Especially since he might be acquitted.

Secret Service agents searched the home of Len Rose, a computer consultant from Baltimore, on May 8. The agents not only seized his computers but confiscated every piece of electronic equipment in the house, including his fax machine, along with some family pictures, several boxes of technical books, and a box containing his U.S. Army medals.

On May 15, Rose was indicted on four counts of wire fraud, aiding and abetting wire fraud, and interstate transportation of stolen goods. Among other things, the indictment alleged that Rose is a member of the Legion of Doom, a claim both he and admitted Doomsters vociferously deny.

The interstate-transportation charge is based on the fact that Rose was in possession of source code for Unix, an operating system used by a wide variety of minicomputers and computer workstations. (Source code is the original text of a program.) In theory, Unix is the property of AT&T, which developed the system. AT&T maintains that Unix is protected as a confidential, unpublished work. In fact, AT&T has sold thousands of copies across the country, and every systems programmer who works with Unix is likely to have some of the source code lying around.

The wire-fraud counts are based on the fact that Rose sent a copy of a "Trojan horse" program by electronic mail. Trojan horse programs are sometimes used by hackers to break into computers; they are also sometimes used by system managers to monitor hackers who try to break in. In other words, a Trojan horse program is like a crowbar: You can use it to break into someone's house, or you can use it to help renovate your own house. It has both legitimate and illegitimate uses.

Rose is a computer consultant and has dealt with security issues from time to time. He maintains that his Trojan horse program was used solely for legitimate purposes—and, in any case, would no longer work, because of changes AT&T has made to Unix since Rose wrote the program. Rose is not charged with actually attempting to break into computers, merely with possessing a tool that someone could use to break in. In essence, the Secret Service found Len Rose in possession of a crowbar and is accusing him of burglary.

By seizing Rose's equipment, the Secret Service has effectively denied him his livelihood. Without his equipment, he cannot work. Rose says he has lost his home, his credit rating and credit cards, his business, and some of his friends. He can no longer afford to retain his original attorney and is now represented by a public defender.

Rose's difficulties are compounded by a theft conviction arising from a dispute with a former client regarding the ownership of computer equipment. Nevertheless, it seems brutal for the Secret Service to deny him the means to support his family and to pay for an effective defense. Investigators must long ago have gleaned whatever evidence his equipment may have contained.

Ultimately, the case against Neidorf and Riggs fell apart. In June, the grand jury issued a revised indictment. It dropped the charges of violating the Computer Fraud and Abuse Act and added seven new counts of wire fraud, some involving electronic mail between Neidorf and Riggs. Neidorf was charged with two counts of wire fraud for uploading issues of *Phrack* to JolNet. In other words, mere distribution of his publication was deemed to be "fraud" because *Phrack* contained material the Secret Service claimed had been obtained by fraudulent means. The new indictment also reduced the "value" of the document Riggs allegedly stole from more than $70,000 to $20,000.

On July 9, Riggs pleaded guilty in a separate indictment to one count of conspiracy in breaking into Bell South's computer. Sentencing was set for September 14—after Neidorf's trial was to begin. Riggs agreed to be a witness for the prosecution of Neidorf.

On July 28, Neidorf's trial began in Chicago. Within four days, it was over. The prosecution's case had collapsed.

Under cross-examination, a Bell South employee admitted that the stolen document was far from confidential. Indeed, any member of the public could purchase a copy by calling an 800 number, requesting the document, and paying $13—far less than the $20,000 claimed value or the $5,000 minimum required to support a charge of transporting stolen goods across state lines.

Testimony also revealed that the contents of the document could not possibly allow someone to enter and disrupt the 911 network. The document merely defined a set of terms used in telecommunications and described the procedures used by Bell personnel in setting up a 911 system.

Riggs, testifying for the prosecution, admitted that he had no direct knowledge that Neidorf ever gained illegal access to anything; that Neidorf was not himself a member of the Legion of Doom; and that Neidorf had not been involved in the initial downloading of the document in any way.

The Secret Service closed down electronic bulletin boards by simply seizing "as evidence" the computers on which they operated.

In short, Neidorf and Riggs had not conspired; therefore, Neidorf should not have been charged with the fraud counts. The only value of which Bell South was "deprived" by Riggs's downloading was $13; therefore, he was, at worst, guilty of petty theft. The interstate-transportation counts were moot, since the "stolen goods" in question were worth less than the $5,000 minimum.

Not only was there no case against Neidorf—there also was no case against Riggs. The government dropped the case against Neidorf. Riggs, however, had already pleaded guilty.

The computer nets do need policing.

Computer crooks can steal and have stolen millions of dollars. But a balance must be struck between civil liberties and the legitimate needs of law enforcement. The laws as currently constituted are inadequate from both perspectives, and the Secret Service seems determined to interpret them with a callous disregard for civil liberties.

To attack computer crime, prosecutors primarily use the statutes dealing with wire fraud and interstate transportation of stolen goods, the Computer Fraud and Abuse Act of 1986, and the Electronic Communication Privacy Act of 1986. The wire fraud statute prohibits the use of the telephone, wire services, radio, and television in the commission of fraud. The courts have, logically, interpreted it to apply to electronic communications as well.

The interstate transportation statute prohibits transportation of stolen goods valued at $5,000 or more across state lines. Neidorf's lawyer moved to dismiss those counts, claiming that nothing tangible is transported when a document is uploaded or downloaded. The judge ruled that tangibility was not a requirement and that electronic transmission could constitute transportation. The Computer Fraud and Abuse Act prohibits knowingly, and with intent to defraud, trafficking in information that can be used to gain unauthorized access to a computer.

The Electronic Communications Privacy Act makes it a crime to examine private communications transmitted electronically. Among other things, it requires law enforcement agencies to obtain search warrants before opening electronic mail. It is unclear whether electronic mail files on a BBS's hard drive are covered by a warrant that permits seizure of the hard drive, or whether separate warrants are needed for each recipient's mail.

The reliance on fraud statutes to fight computer crime presents problems. Fraud is the use of chicanery, tricks, or other forms of deception in a scheme to deprive the victim of property. Most attempts by hackers to gain illegal access to a computer do involve chicanery or tricks, in some sense—the use of other people's passwords, the use of known bugs in systems software, and so on. Much of the time, however, a hacker does not deprive anyone of property.

If the hacker merely signs on and looks around, he deprives the computer operators of a few dollars of computer time at worst. If he downloads a file, the owner still has access to the original file. If the file's confidentiality has value in itself—as with a trade secret—downloading it does deprive the owner of something of value, but this is rarely the case.

We need a "computer trespass" statute, with a sliding scale of punishments corresponding to the severity of the violation. Just as burglary is punished more severely than trespass, so a hacker who steals and uses credit card numbers ought to be punished more severely than one who does nothing more than break into a computer and examine a few public files. In the absence of such a scheme, law enforcement personnel naturally try to cram all computer violations into the category of fraud, since the fraud statutes are the only laws that currently permit prosecution of computer crimes. As a result, petty crimes are charged as felonies—as with Neidorf and Riggs.

Legitimate users and operators of com-

puter networks need to be protected from arbitrary seizures and guilt by electronic association. The criminal code permits law enforcement personnel to seize equipment used in a crime or that might provide criminal evidence, even when the owner has no knowledge of the crime. But the purpose of such seizures is to allow the authorities access to evidence of criminal activity, not to shut down businesses. Searchers need not remove computer equipment to inspect the files it contains. They can sit down and make copies of whatever files they want on the spot. Even if they expect some piece of incriminating material to be

hidden particularly well—for example, in a specially protected file or in a ROM chip—it is unreasonable to hold onto the seized equipment indefinitely.

And it's clearly wrong to seize equipment that cannot, by any stretch of the imagination, contain incriminating data. In both the Steve Jackson and Ripco cases, the Secret Service seized laser printers along with other equipment. Laser printers have no permanent memory (other than the factory-supplied ROM chips that tell them how to operate). They print words on paper, that's all. They cannot contain incriminating information.

Even computers themselves cannot possibly constitute evidence. When you turn off a computer, its memory dies. Permanent data exist only on storage media—hard drives, floppy disks, tape drives, and the like. Even if law enforcement personnel have some compelling reason to take storage media away to complete a search, they have no reason to take the computers that use those media.

Just as a computer is not evidence because it once carried incriminating information, a network is not a criminal enterprise because it once carried data used in or derived from fraudulent activity. Yet under current law, it seems that the operator of a bulletin board is liable if someone posts an illegal message on it. Say I run a BBS called Mojo. You dial Mojo up and leave Mario Cuomo's MasterCard number on the board, inviting anyone to use it. Six people sign on, read the message, and fly to Rio courtesy of the governor before I notice the message and purge it. Apparently, I'm liable—even though I had nothing to do with obtaining Cuomo's credit card number, never used it, and strenuously object to this misuse of my board.

Such an interpretation threatens the very existence of the academic and commercial nets. A user of UseNet, for instance, can send a message to any other user of UseNet. The network routes messages in a complex fashion—from Computer A to Computer B to Computer C, and so on, depending on what computers are currently live, the volume of data transmitted among them, and the topography of the net itself. The message could pass through dozens of computers before reaching its destination. If someone uses the message to commit fraud, the system operators of every computer along its path may be criminally liable, even though they would have no way of knowing the contents of the message.

Computer networks and BBSes need the same kind of "common carrier" protection that applies to the mails, telephone companies, and wire services. Posting an illegal message ought to be illegal for the person who posts it—but not for the operator of the board on which the message appears.

The main function of the Net is to promote communication. People use it to buy goods, research topics, download software, and a myriad of other things as well, but most of their computing time is spent communicating: by posting messages to bulletin boards, by "chatting" in real time, by sending electronic mail, by uploading and downloading files. It makes no sense to say that discussion of a topic in print is OK, but discussion of the same topic via an electronic network is a crime.

Yet as currently interpreted, the law says that mere transmission of information that someone *could* use to gain access to computers for fraudulent purposes is itself fraud—even if no fraudulent access takes place. The Secret Service, for instance, was willing to indict Neidorf for publishing information it thought could be used to disrupt the 911 network—even though neither Neidorf nor anyone else actually disrupted it. We must clearly establish that electronic communications are speech, and enjoy the same protections as other forms of speech.

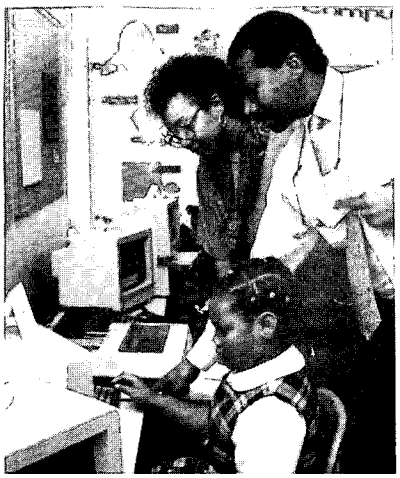
The prospects for such legal reform are not bright. Three times in this century, technological developments have created new venues for speech: with radio, with television, and with cable. On the grounds of scarcity, government restricts freedom of speech on radio and television; on the grounds of natural monopoly, government regulates speech on cable. Recent events, such as the conviction of former Cornell graduate student Robert T. Morris for introducing a virus into the nationwide ARPANet, have aroused worry about hacker crimes. But concern for the rights of legitimate users of computer nets has not received the same level of publicity. If anything, recent trends lean toward the adoption of more draconian laws—like the Computer Fraud and Abuse Act, which may make it illegal even for computer security professionals to transmit information about breaches of security.

The Net is vast—and growing fast. It has already changed the lives of thousands, from scientists who learn of new breakthroughs far more quickly than if they had to wait for journal publication, to stay-at-home writers who find in computer networks the personal contact they miss without office jobs. But the technology is still in its infancy. The Net has the capacity to improve all our lives.

A user of the Net can already find a wide variety of information, from encyclopedia entries to restaurant reviews. Someday the Net will be the first place citizens turn to when they need information. The morning paper will be a printout, tailored to our interests and specifications, of articles posted worldwide; job hunters will look first to the Net; millions will use it to telecommute to work; and serious discussion will be given to the abolition of representative government and the adoption of direct democracy via network voting.

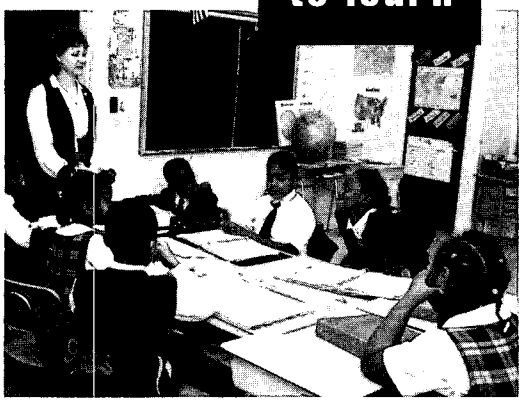
Today, we are farmers standing by our country lanes and marveling as the first primitive automobiles backfire down the road. The shape of the future is murky. We cannot know what the Net will bring, just as a farmer seeing a car for the first time couldn't possibly have predicted six-lane highways, urban sprawl, the sexual revolution, and photochemical smog. Nonetheless, we can see that something remarkable is happening, something that will change the world, something that has the potential to transform our lives. To ensure that our lives are enriched and not diminished, we must ensure that the Net is free. ■

Greg Costikyan is a writer of fiction and nonfiction who has designed 23 commercially published games.



The church-affiliated Monroe Saunders School in Baltimore has a calm, scholarly atmosphere.

How do you get kids to learn



and parents to care?

STRENGTH

The Monroe Saunders School in Baltimore and the Sheenway School and Culture Center in Los Angeles are separated by more than just 3,000 miles and three time zones. Located on a 22-acre campus of grassy, rolling hills in the suburban outskirts of Baltimore, Monroe Saunders School inhabits a stately, multi-story brick building that once housed a preppy boarding school for girls. Its 80 K-3 students wear uniforms, come from primarily middle- or upper middle-class professional families, and attend a school with a clear and undeniable religious setting. The school's parent church, the worldwide First United Church of Jesus Christ-Apostolic, absorbs some of the school's costs.

Sheenway inhabits a small complex of single-story units on the outskirts of Watts. The carpet in its reception area is held together with gray duct tape. Its 80 students come from both working- and middle-class families, some intact with two parents, some with only a mother. Its teachers use the Montessori and Socratic methods, and students progress without rigid class times or grade categories. With no sponsoring church for support, Sheenway must supplement tuition income with donation drives, car washes, bake sales, and many volunteer instructors.

But there are important similarities between Saunders and Sheenway. Both charge under $3,000 a year in tuition, less than what is spent per pupil at nearby public schools. Both produce students who attend college or professional schools in significant numbers. Both began as the vision of a single, entrepreneurial family. Both eschew government aid. And both are operated by and for black Americans.

It is the differences between Saunders and Sheenway—determined by their communities, their founders, and their philosophies—that suggest a solution to the nation's education crisis. In America's successful black private schools, no single approach seems to work best. Autonomous schools, diverse in program and personnel, meet the varying needs of students and parents. If the experience at Saunders, Sheenway, and other schools is any guide, education-reform efforts that rely on state mandates and higher spending are doomed. Diversity is the key to quality.

Black private schooling is a widespread but relatively little-known phenomenon. Joan Davis Ratteray—whose Institute for Independent Education in Washington, D.C., has identified, studied, and publicized black and other minority private schools for half a decade—speaks of an "Underground Railroad in minority education" that allows the "slaves" of failed public schools to "escape to freedom." Like its Underground Railroad precursor, America's network of black private schools can offer services to only a small percentage of the population, but news of the network's success, spread by family ties and word of mouth, inspires many other blacks. And just as the Harriet Tubmans of the Underground Railroad pursued their visions of freedom with tireless effort and personal devo-

TOM JEMSKI