12/92

; Mixing Sound Are on the Way

. with bells ndus- case, l two ır an- a re- res to of the multi- on of ıputer me. I . Four same a. It's of my bea tech e pro- ıdows, s onto of the radio n play s nifty. ıten to of the some ısers – e such rest of arrive presi- velop- lls the music sed to he ar- ıurated ushing effects ecialty es a e com- ational shed a) More ısiness

software is also moving in that direction but at a slower pace, Mr. Gupta concedes. With sound-board prices down from $1,000 to about $200 or $300, he predicts more people will try out talking computers.

You can talk back too. Some programs now control computers by voice command. But don't rush into that technology just yet. When InfoWorld tested three such systems recently (one each on a PC, a Macintosh, and a Next machine), it found none of them quite up to expectations.

At the moment, sight, not sound, seems to be driving the multimedia market. Michael French, senior consultant with Link Resources, says most buyers are going to multimedia for better images – everything from animation to still photography to moving pictures.

The market for these technologies is still small. Link estimates that only 9 percent of the office computers shipped last year were multimedia ready. (It was only 1 percent for home computers.) That should change by mid-decade. In 1996, the company forecasts that 75 percent of all office machines and 65 percent of all home computers will be multimedia ready.

Of course, being multimedia ready doesn't come cheap. The technology requires a fast computer, lots of memory, and loads of hard-disk space. My CompuAdd computer was built around a Cyrix 486 chip with three megabytes of random-access memory and a 120-megabyte hard disk. (Total cost: $3,354.13) At times, the machine didn't quite keep up when I was recording speech at the highest quality levels. Look for multimedia machines with larger hard disks (200 megabytes or more), at least eight megabytes of memory, and faster processors.

So I'm moving slowly into this technology. My first investment will undoubtedly be a CD-ROM drive, the fastest one I can get. My CompuAdd experience has convinced me that CD-ROM is just too useful to pass up. It delivers volumes of information quickly to people like me who spend hours on their computers.

Does that make me multimedia ready? Not quite. Call me "multimedia-expectant."

– Laurent Belsie

■ *Send your comments on this column to CompuServe (70541,3654) or Prodigy (BXGN44A).*

Hunting Computer Hackers

By Simson L. Garfinkel

TWO years ago, the United States Secret Service declared war on the computer-hacker underground. In a series of well-coordinated raids around the country, law-enforcement agents broke into suburban homes – guns drawn – and presented unsuspecting parents with search warrants for their teenagers' computers. When it was over, "Operation Sundevil" had seized more than 40 computer systems and 23,000 floppy disks.

Although most of the computers seized were never returned, few of the seizures actually resulted in arrests and prosecutions. The purpose of Operation Sundevil, asserts noted science-fiction author Bruce Sterling in his first nonfiction work, "The Hacker Crackdown: Law and Disorder on the Electronic Frontier," was to send a message to computer hackers everywhere.

The message: Law enforcement would no longer stand by while high-school students rerouted calls in the nation's phone system and stole reports from credit databanks. As an added benefit, Sundevil seized the instruments of these minors' crimes without forcing the federal bureaucracy to go through the formalities of trials and convictions.

What nobody in the law-enforcement community expected, Sterling writes, was that an organized group of well-financed adults would come to the rescue of these computer criminals.

An assembly of civil libertarians, founded by Lotus millionaire Mitch Kapor and Grateful Dead lyricist John Perry Barlow, is now known as the Electronic Frontiers Foundation. It is but one of many organizations whose birth and growth is chronicled by "The Hacker Crackdown."

In writing about the events leading up to Operation Sundevil and their aftermath, Sterling also tells interesting, although somewhat spotty, histories of the US telephone system, the US Secret Service, and a variety of state and federal agents who have devoted their careers to the prosecution of computer crime. With access that is rarely granted to journalists, Sterling takes readers on a tour of the US government's 1,500-acre Federal Law Enforcement Training Center in Glynco, Ga., and then to a meeting of the government's Federal Computer Investigations Committee.

But the bulk of the book is devoted to Sterling's account of the hacker underground – the real-life world of cyberpunks and cyberspace. He has a flair for writing about these genuinely curious youngsters whose principal joys in life seem to be exchanging information about building explosives, breaking into telephone company computers, and spreading the gospel of anarchy.

Sterling walks a careful line between police, who, he asserts, believe that all hackers are thieves, and the hackers, some of whom actually are thieves. He is generally unmoved, though, by law-enforcement claims that hacking will soon cost lives as these teenagers move on from mastering the emergency 911 system to rerouting Amtrak trains and playing with the national air-traffic-control system.

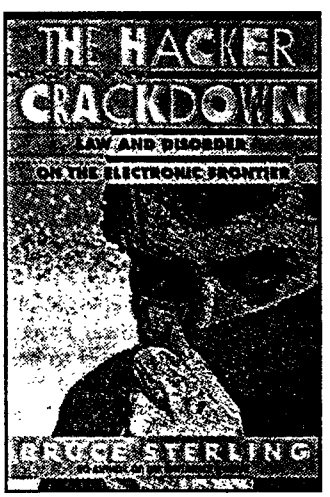
"Consider this," he writes. "If 'hacking' is supposed to be so serious and real-life and dangerous, then how come *nine-year-old kids* have computers and modems? You wouldn't give a nine-year-old his own car, or his own rifle, or his own chainsaw."

Sterling spends nearly a quarter of his book providing solid technical background on the phone system and its vulnerabilities, both technical and administrative. He gives readers real-life examples of "trashing" (searching through trash cans for damaging information) and "social engineering" (ways that hackers convince telephone company officials to do their bidding). Ironically, the book is an excellent starting point for hackers in training.

Sadly, Sterling's work lacks accuracy on many details. For example, he gives the erroneous impression that after the hacker crackdown of 1990, law-enforcement officials learned their lesson and stopped seizing computer bulletin-board systems. He also fails to criticize his heroes, the civil libertarians, although finding such criticism in the law-enforcement community isn't difficult. "The Hacker Crackdown" is a good read, but a bad starting point for setting public policy.

■ *Simson L. Garfinkel is a freelance writer who specializes in science and technology.*

BOOKS



THE HACKER CRACKDOWN: LAW AND DISORDER ON THE ELECTRONIC FRONTIER
By Bruce Sterling
Bantam Books
328 pp., $22.50