phone lines have melted, as they did in Hinsdale. "Nobody had really focused on the lack of redundancy in the Bell operating companies' networks," notes Hipp. Local phone companies relay computer signals to a long-distance carrier such as American Telephone & Telegraph Co. or a data network such as Tymnet, which relays the signal to a local phone company that picks it up for the customer. Without that last link, the most sophisticated computer network may be useless.

Most of the time, phone company backup systems route calls around trouble spots. But in Hinsdale, a worst-case scenario occurred. The automated phone switching facility was unstaffed and lacked the kind of fire-suppression system used in computer centers. There was no alarm at the local fire station, because Illinois Bell feared that the fire department couldn't put out a computer fire without causing excessive damage.

The result: Thousands of homes and businesses, including headquarters offices of McDonald's Corp. and Motorola Corp., were cut off. Large businesses restored communications with emergency microwave radio systems. But seven local businesses have filed lawsuits to recover losses caused by the outage.

Computer customers, as well, want better security features from hardware and software suppliers. Many companies are considering making AT&T's Unix software—or its derivatives—a standard to smooth the connections between different brands of machines. But since Unix was designed to make it easy for computers to share files and programs, it's also susceptible to break-ins, says Judith S. Hurwitz, editor of *Unix in the Office*, a newsletter.

For instance, phrackers in California, after cracking the password system on

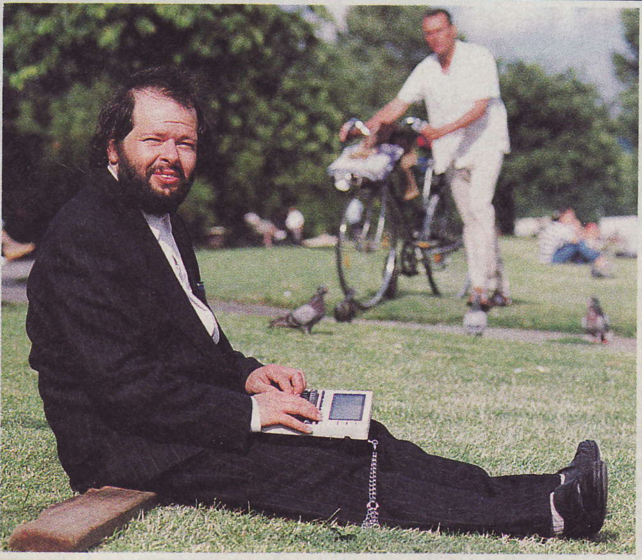
A GERMAN HACKERS' CLUB THAT PROMOTES CREATIVE CHAOS

West German computer hacker Bernd Fix holds the economic equivalent of a nuclear bomb in his head. The University of Heidelberg astrophysics student claims it took him only 20 hours to write a virus that could destroy all information in a mainframe computer—erasing tens of thousands of pages in minutes. In the wrong hands, it could cripple companies, the IRS, even the Pentagon. Fix has no such plans: He says he wrote the program as an intellectual exercise—"for the experience of doing it." He has since encrypted it so that it can't be used by others.

Welcome to the oddball world of hacking, German style. Fix, 26, is a member of the Hamburg-based Chaos Computer Club, a group of 300 hackers who, says Herwart "Wau" Holland, the club's founder and leader, are a far cry from the teenage thrill-seekers who prowl U.S. computer networks. Despite the club's name, Holland, 36, says it's against electronic mischief. His goal is more serious: increasing the flow of public information. In West Germany, environmental and scientific data, census figures, and government reports are costly and difficult to get. "It's not a very democratic system," Holland says. Not until Chaos gets involved.

Holland's weekly newsletter, circulation 3,000, and his "Hacker's Bible," 25,000 copies sold, are filled with tips on breaking into computer systems around the world. "We believe we have the right of access to information, and we take it," says Holland. During the Chernobyl nuclear disaster, he says, German officials "fed the public a lot of false [reassuring] statements." By purloining hidden data, "we made sure the press was well informed"—a claim that German reporters confirm.

FORBIDDEN FUN. Chaos members, who meet weekly, hold an annual convention, and pay dues of $66 a year, revel in showing up West Germany's obstinate bureaucracies. In 1984, Chaos uncovered a security hole in the videotex system that the German telephone authority, the Deutsche Bundespost, was building. When the agency ignored club warnings that messages in a customer's private electronic mailbox weren't secure, Chaos members set out to prove the point. They logged on to computers at Hamburger Sparkasse, a savings bank, and programmed them to make thousands of videotex calls to Chaos headquarters on one weekend. After only two days of this, the bank owed the Bundespost $75,000 in telephone charges. Uncaught, Chaos revealed its stunt on Nov. 19, the birthday of Bundespost Minister Christian Schwartz-Schilling. Both the bank and the Bundespost now say the break-in was a fluke.



HOLLAND: "WE HAVE THE RIGHT OF ACCESS TO INFORMATION"

BOSSU/SYGMA

The incident fits with Holland's goal "of changing structures in society. Everything in Germany is so overly organized." He adds: "Some people throw bombs. It's more effective to find the absurdities and make people laugh."

Like hackers everywhere, however, Chaos members can't resist a challenge. And that sometimes means treading near the edge of West German law, which prohibits manipulating or destroying data, both foreign and domestic, or breaking into "extra secure" systems, which are undefined. Holland denies that the club was behind a NASA break-in last year. Chaos members may have done it, he concedes, though none has confessed. But he adds: "We do not encourage illegal acts."

That's an assertion that critics often discount, given the club's key role in promoting hacking—and its record of never having expelled anyone for unsportsmanlike conduct. Still, Holland, who traded his blue jeans for blue suits when he started a typesetting business 18 months ago, knows that hacking can hurt. Three years ago, fellow enthusiasts stole his password to a German data network and published it in the tabloid *Bild Zeitung*. Soon gleeful computer fanatics had racked up $1,500 in charges to Holland's account. "I was broke at the time, and this incident made an impression on a lot of hackers who knew me," he says.

Nonetheless, there's still the matter of all that closely held government information. And until it's more public, Chaos most likely will fill the void.

By Gail Schares in Heidelberg