The Associated Press June 30, 2002

Security analysts dismiss fears of terrorist hackers Electricity, water systems hard to damage online

By Bill Wallace, Chronicle Staff Writer

Despite growing government concern that al Qaeda and its allies may try to use computers to disrupt electrical power grids and transportation systems, many experts on terrorism and computer security are skeptical about the overall menace of cyber-terrorism. Cyber-terrorism has become one of the hottest buzzwords among national security officials, especially since the Sept. 11 attacks.

However, "it is unlikely that somebody with a laptop in Pakistan, could bring down California's power grid," said Kevin Terpstra, who works as communications director for the California Department of Information Technology (an agency which is responsible for assessing the security of the state's computer systems.)

"There is reason to be concerned about computer security and critical infrastructure vulnerabilities . . . but the likelihood of this type of an attack is very small."

In January, the FBI's National Infrastructure Protection Center warned that information on the Internet about power plants, toxic waste dumps and other sensitive sites could be used by foreign extremists to launch attacks on the United States.

And last week, the Business Software Alliance, a trade association, released an industry survey in which 59 percent of the information technology specialists polled said they considered a major terrorist computer attack likely in the next 12 months.

Underscoring the possible danger, several newspapers reported that computer operators in the Middle East and South Asia had attempted to penetrate computer systems in Northern California last fall.

However, experts interviewed by The Chronicle said the vast majority of these computer intruders are trying to steal information -- not shut down electrical utilities, release water from dams or engage in other dangerous acts of sabotage.

It is difficult, the experts say, for a hacker to launch an attack on an infrastructure control system because very few of these systems are accessible through the Internet.

In March, CIO magazine, a journal for computer system professionals, published a detailed article on information security that debunked the cyber- terrorist threat.

The magazine quoted Marcus Kempe, the director of operations for the Massachusetts Water Resource Authority, as saying a cyber-terrorist intent on tampering with his utility would have to make three complicated intrusions to gain access to the necessary control systems.

And he would have to break into a highly secure building in Massachusetts in order to make them because the system is not connected to the Internet. This would present a problem for the terrorist who thinks he can sabotage the utility by using his laptop in Pakistan.

"Could a computer attack get us to a high-consequence event? Probably not," Kempe told the magazine.

David Wagner, a computer science professor at UC Berkeley who specializes in information security, said some utilities do have operations that are controlled by means of the Internet, "but not all of them and maybe not the most critical ones."

"There are some crucial vulnerabilities," Wagner said, "but if you want to rank how serious those vulnerabilities are, they are less serious than what you can do with explosives and much less serious than what you could do with chemical or biological agents.

"I used to be concerned about cyber-terrorism, but I think in the past year I have come to realize that it is not the most serious thing we have to worry about."

Dorothy Denning, the director of the Georgetown University Institute for Information Assurance, testified before the House Judicial Committee two years ago that cyber-terrorism, while worthy of concern, was overrated as a threat to the American public. Denning told The Chronicle that her opinion has changed little since the Sept. 11 attacks.

"To get noticed, they would have to do something very dramatic, like flood a dam or something," she told The Chronicle. "Those kinds of actions are a lot more difficult to engineer with a computer than they would be with a bomb -- and whether they would work or not would be a lot less certain."

John Pike, a weapons systems analyst and director of Globalsecurity.org, a defense policy organization in Washington, D.C., stressed that terrorists use simple, direct methods for operations because they are less likely to fail.

He said the Sept. 11 attacks were a perfect example. "You had 20 people get on four planes to attack two targets," he said. "Only 19 made the flights, and only three of the planes reached their targets. But the plan succeeded anyway because it was simple."

He said cyber-attack scenarios are too complex to have much appeal for terrorist groups. Furthermore, they are likely to fail.

"If you pitch a bad script in Hollywood, the worst that can happen is you get thrown out of the office," he said with a chuckle. "If I were some guy from al Qaeda pitching a (complicated and risky) cyber-terrorism plot to Osama bin Laden, I would be a little nervous about making it out of his office alive. "