Wiretap 'Pro's' View Democrats' HQ 'Bugs'

By Ronald Kessler
Washington Post Staff Writer

Experts skilled in the art of wiretapping and bugging say each has his own preferred techniques for carrying out their appointed missions, but that none of the methods bears any resemblance to those used a week ago yesterday in the abortive bugging attempt at Democratic National Committee headquarters.

Although the methods favored by the professionals differ, the common thread running through all of them is that they are calculated to provide reliable, high-quality voice transmission using the simplest and smallest available devices to minimize the risk of detection.

A look at some of these methods—all illegal except when carried out by law enforcement officers armed with court orders—provides some insight into the current state of the art of wiretapping and bugging.

"This is a results-oriented business," says one old-time professional. "You don't get paid for building exotic devices. You get paid for conversations," he says.

Considerable publicity has been generated by bugging devices hidden in martini olives or highly sophisticated bugs that don't require physical entry into the premises to be bugged.

One, said to be developed by the Central Intelligence Agency, trips a switch in a standard telephone to make the instrument an open microphone, transmitting room conversations and telephone calls down the telephone wire to monitors miles away. The switch is tripped by placing a radio frequency wave on the telephone wire at any location outside the home or office being bugged.

Another device, still being developed by government intelligence agencies, uses a laser beam to "read" sound vibrations bouncing off window panes. The sound waves from the windows modulate the light waves from the laser, and the modulated light waves are translated back into sound.

A third device, once implanted in a telephone, can be activated from anywhere in the world by simply dialing the number of the telephone and placing a tone of a specific frequency on the line.

Each of these devices has drawbacks, not the least of which is that the clarity of transmission doesn't compare with that of more conventional bugs planted in side the premises where the conversations are taking place.

"When you go into this, you have to do it right, and that means breaking and entering," says Allan D. Bell Jr., a former high-level military intelligence wiretapper and debugger who has worked with the CIA and Federal Bureau of Investigation on bugging matters.

Bell, who heads Dektor Counterintelligence & Security Inc., a Springfield manufacturer of de-bugging devices, says that if he were assigned to bug the Democratic headquarters, he would probably choose from one of three approaches.

If only a few days of listening were needed, Bell says, he would conceal a fully self-sufficient radio transmitter the size of a sugar cube under a conference table or desk. The beauty of such a device, he notes, is that the one responsible for installing it generally cannot be apprehended unless caught in the act.

For more permanent installations, he says, he would wire a telephone in the room to be bugged so that it becomes an open microphone. The room conversations and telephone calls would be transmitted through a third, spare wire in the telephone equipment to a remote listening post, perhaps miles away.

A third possibility, he says, would be a radio transmitting device hooked up to the electric current in a home or office. The device would be implanted in an electrical fixture, such as a lamp, or could be manufactured as part of a dummy electric outlet wall plate, detectable only by x-ray.

The device would operate permanently on household current and would beam low-frequency waves along the power lines to be picked up by the eavesdropper at any point along the line. Because the radio signal would be generally confined to the power line, Bell says, it would be difficult to detect its presence through conventional de-bugging methods.

Another wiretap expert is Michael J. Morrissey, chief engineer of B. R. Fox, Inc., a Holmes, N. Y., de-bugging company formerly headed by the late Bernard Spindel,

who was considered by federal authorities to be the top wiretapper in the country.

Morrissey says he would plant a combined microphone and amplifier the size of a pinhead somewhere along the telephone line or inside the telephone in a room to be bugged. The signal would be led off through the spare wire that comes with most telephone equipment, he says.

Morrissey says he might plant additional pinhead-size microphones in other parts of the room and connect them to the amplifier with invisible electrically conductive fluid painted on the walls or with gold wire thinner than a strand of human hair.

Morrissey, who teaches a course in wiretapping and bugging for law enforcement agencies, says it is important that radio transmitter bugs have the capability of being turned off remotely by the listener so that the signals cannot be detected by de-bugging devices.

"When you hear the debugging people come in, that's when you pull the switch," Morrissey says.

Another bugging expert, with years of experience working for private parties and government agencies, says any premises to be bugged nust be "cased" for several weeks before a break-in attempt is made. Only one man actually enters the room to be wired for sound and installs the devices, he says, but several men are planted outside the office and outside the building to warn the installer by pre-arranged signals if police, burglar alarm dispatchers or security grards drive up.

"The man outside acts like he's drunk or makes up some story or excuse. A minute's delay is all the installer needs to get away," he says.

The men involved never take a room near the bugging scene, the expert says. Instead, two girls are hired to move into a room nearby, and they tape-record the conversations beamed by the radio bugs, he says.

"Girls are the perfect decoy," he says. "No one suspects them, and the equipment is kept in a suitcase that the police can't search without a warrant. This is the way the pros do it," he says.