New Bug-Killer Developed to Foil Secret Telephonic Super-Snooper

10-1-71

By Ronald Kessler
Washington Post Staff Writer

A group of former military intelligence wiretap experts say they have developed a method of counteracting a still-classified bugging device that transforms any telephone into an open, transmitting microphone.

Even the name of the recently publicized bugging device is classified, they said, and declined to reveal it.

The experts, who say they have worked with the Central Intelligence Agency and Federal Bureau of Investigation on electronic surveillance, said the secret device was developed by government intelligence agencies more than 10 years ago, and they described as accurate a Washington Post story last Friday disclosing the existence of the device.

What is unique about the device, the story quoted Clyde Wallace, a manufacturer of bugging equipment, as saying, is that it bugs and taps from remote locations without the need to physically enter the premises and install any listening equipment.

Wiretapping is interception of telephone calls, while bugging is surreptitious eavesdropping on room conversations with the help of electronic aids.

The device, Wallace told a group of federal law enforcement and security investigators, can be placed anywhere on a telephone line, on a telephone pole, inside a cable vault, or in telephone company switching offices. Or it can be connected to leased lines that permit monitoring of conversations from secret rooms.

See BUG, C8, Col. 1

BUG, From C1

The device places a radio frequency wave on the line. The wave activates a switch in the telephone to be bugged, permitting sound waves from the room where the phone is installed to be transmitted down the telephone line from the telephone mouthpiece, even when the receiver is on the hook.

According to Wallace, two federal agencies are already using the device. Both the CIA and FBI declined to comment last week on whether they are the agencies.

The former military intelligence experts, who have formed a company to manufacture bugging and debugging equipment, said the countermeasure they have developed against the secret bug has been tested on it and is effective, although they said they do not currently have the bug in their offices.

The company, formed last June, is Dektor Counterintelligence and Security, Inc., in Springfield. Four of its officers have extensive backgrounds in installing and detecting bugs and taps in the military. One of the officers, Arnold E. Preston, was a senior instructor and researcher in telephone countermeasures at the Army Intelligence School at Ft. Holabird, until he joined the company last spring.

Allan D. Bell Jr., president of Dektor and holder of more than half its stock, retired in 1968 as a lieutenant colonel after 15 years in military intelligence and counterintelligence, including work on security matters in the office of the Secretary of Defense.

On his resume, Bell, 44, lists 12 military decorations and awards, 37 publications on intelligence and security, and 11 James Bond-like inventions given to military intelligence, including concealed lock-picking equipment and vehicle surveillance devices.

One invention Bell, through his company, is marketing is a device to detect lies by electronically measuring the voice of the subject as he tells a lie. The device would permit checks on truth or falsehood without the knowledge or permission of the subject.

Bell and his colleagues left military intelligence, they say, because of frustration with what they call the slow pace of implementing their bugging and debugging discoveries.

Bell wouldn't say how frequently the government may use the secret bugging device or whether even more sophisticated devices have been developed.

"My career through the years has been keeping my mouth shut," Bell, smiling, said.

Eavesdroppers do not necessarily use the most sophisticated devices available, Bell said. "When a person goes on a bugging job, his choice of devices is based on such factors as importance of clarity, amount of time the bug will be in use," need for undetectability, and the accessibility of the area," he said.

If a room can be entered to install a bug, it generally will be, Bell said, for the sake of clarity. One of the

Ret to HW

'Bug-Killer' Foils Super-Snooper

best places to do the bugging is in a telephone, because it is usually in a central location for the clearest pick up of conversation and comes equipped with its own power and wires leading outside.

By bugging a phone, the eavesdropper can intercept both telephone calls and room conversations. The most "interesting" conversations, Bell said, are those that occur within five minutes after the subject has finished a telephone call. During this time, Bell said, he may tell an associate or a secretary what he really thought of the person he was talking with.

There are some 12 ways to bug a phone, most of them requiring some alteration of the instrument itself. Some can only be detected by taking X-rays of the phone, Bell said.

Bell said any of the methods including the secret bugging device that does not require alteration of the phone can be foiled with Dekton's Telephone Security Device, a neat box that fits under the telephone.

What is does is quite simple. It disconnects the phone and stops all signals in it.

Many security agencies instruct employees in sensitive jobs to manually unplug their telephones from wall jacks when they are not in use, Bell said. A separate bell signals the user that he has a call, and he then connects the phone.

There is a problem with this clumsy method, Bell said: The bell itself can be used as a bug.

What happens, he explained, is that the wires coiled around the field of a permanent magnet in the bell vibrate when sound waves strike them, and these vibrations can be transmitted down the telephone wire to create an effective bug.

The Dektor device, which costs $100 for a single line telephone and $477 for a five-line model, eliminates this problem, Bell said, by supplying independent electrical current—rather than telephone system current—to the bell, cutting off any connection between the bell and the telephone line. The bell is activated by a light rather than an electrical switch, eliminating the possibility that the switch could be bypassed with radio waves, Bell added.

The device cuts off the remaining telephone connections both physically, with a switch, and electrically, by short-circuiting all 50 separate connections that are housed in a five-line telephone.

The security device does nothing to prevent eavesdropping while the telephone is being used, Bell said. There are only two ways to prevent interception of the call itself: foregoing telephone calls, and using expensive scramblers on both ends of the conversation, he said.