ON PAGE 22

TIME
20 April 1987

The Art of High-Tech Snooping

How nigh-invisible devices can get under an embassy's skin

For the past several weeks, American technicians have been feverishly searching the U.S. embassy in Moscow for bugs that might have been planted by Soviet agents let in by Marine guards. So far, they have found nothing tangible. "Not a microphone, not a transmitter, not even a wire," says one knowledgeable source.

Reassuring? No, chilling. American experts are virtually certain that the bugs are there, all right, but are so tiny and cleverly hidden that they are next to impossible to uncover. Sources familiar with the situation say technicians have detected audio-frequency emissions that they think originate in the electronic-coding equipment. That suggests a device in the equipment that enabled the KGB to read the plain-English versions and then the coded versions of messages, and thus crack U.S. codes and read American diplomatic cables throughout the world. Moreover, inspections of the new U.S. embassy building now under construction have turned up plenty of signs of bugs: cables seemingly unconnected to anything, odd indentations in wall panels, steel reinforcing rods so arranged as to convert structural pillars into antennas.

To American experts, the moral of these Moscow mysteries is distressingly plain: the U.S.S.R. may be deficient in many areas of high technology, but its spying techniques are as sophisticated as its missiles. Says former Defense Secretary James Schlesinger, who has been deputized by the State Department to figure out whether the new embassy can ever be made secure: "The notion that the Soviets are a decade behind the U.S. [in technology] certainly does not apply to electronic snooping." The U.S. is probably ahead in the art of miniaturization, but the Soviets have more experience in applying new technologies to snooping. A CIA veteran suggests, only half jokingly, "Judging by what they are producing, the Soviets spend as much on technical bugging as they do on their space program."

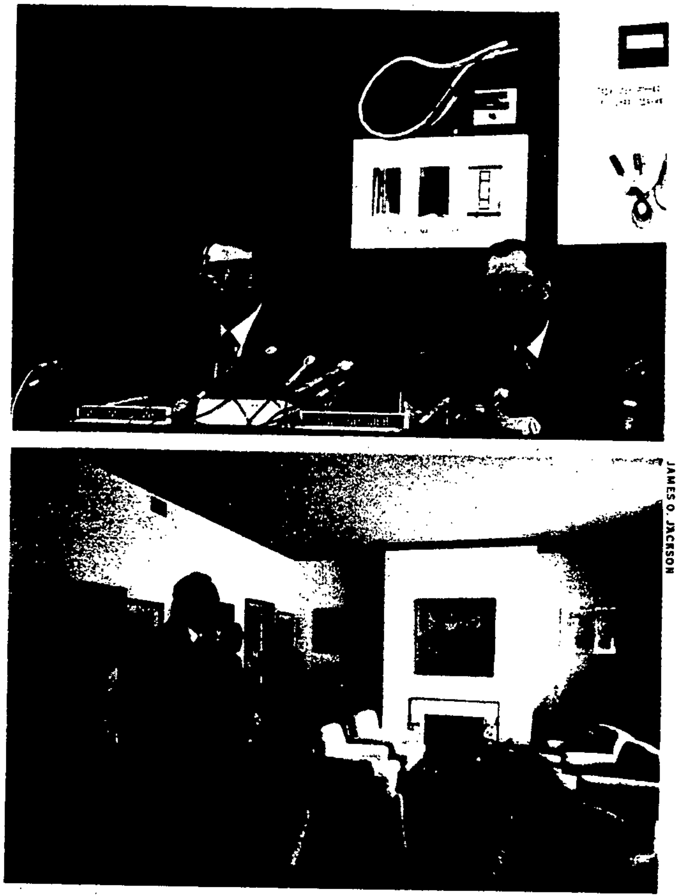
How state-of-the-art spying techniques work is the province of only a few people in the innermost recesses of the KGB and the CIA. Moreover, U.S. counterintelligence experts have an uneasy suspicion that the Kremlin may have come up with devices that they are not yet aware of. Executives in private companies that produce snooping equipment for the U.S. Government are under strict orders to keep their mouths shut, but they do provide some insight into the weird world of electronic espionage and its impressive technology.

Microphone-transmitters these days can be made about the size of a pinhead and embedded anywhere (or everywhere) in a wall, ceiling, chair or a person's clothing. Some do not need wires to transmit; they send out microwave signals that can be read by equipment outside the building. They can be turned on and off by remote control, or set to be activated by heat, radiation, the vibrations of a voice or pressure. A bug in a chair might turn itself on when someone sits down.

These bugs are devilishly difficult to detect, and not just because of their tiny size. A standard method of finding bugs is the electronic "sweep." A device beams microwaves at the entire surface of, say, a suspect wall; a bug struck by the microwaves emits a telltale signal, but only if it is transmitting. Newer bugs can record data for perhaps 15 seconds, then transmit all of the stored information in a single burst lasting a microsecond. Unless a detection device beams microwaves at the bug during that microsecond, the listening gadget will not be found.

In a computer age, methods of foiling the bugs do not always work. A hoary staple of spy fiction is the conversation conducted in low tones with a radio blasting loud music and faucets running splashily in the background. But if the sounds are picked up by several bugs scattered around a room, a computer can compare the sound tracks from different angles, pick out the voice vibrations and edit out other noise. Says one specialist in computer enhancement who has worked for U.S. Government agencies: "A voice on a tape that is completely obscured can be reproduced so that you hear only the voice and hardly anything else."

Bugs can also be hidden in electric typewriters, printers and similar machines. They pick up and transmit the electronic signals given off by each key or by the ball in a Selectric-style typewriter. Someone receiving the transmissions outside the building can read the message almost as easily as if he were looking over the typist's shoulder. American inspectors found bugs in a shipment of typewriters delivered to the Moscow embassy two years ago. But did they get all? It is common practice for buggers to leave some devices that are sure to be found in order to engender a false sense of security in the finders.



Counterclaims: the Soviets display what they say are U.S. snooping devices planted in their missions. Former U.S. Ambassador Arthur Hartman shows off the new, bug-infested Moscow embassy

JAMES O. JACKSON

One way to make bugs hard to detect is to disguise or hide the radio frequencies of their transmissions. This can be done by having them send their data on frequencies that are very close to those used by standard radio or TV broadcasts, a technique known as "snuggling." Another method is to "frequency hop" across a broad spectrum by transmitting for a millisecond at one frequency, then another, then another.

Especially hard to detect are bugs that do not transmit through the air. Instead,

Continued

they are attached by wires to a listening post outside the building. The connecting "wires" can be almost anything that conducts electricity: metallic paint under the surface paint of a room, a regular electric line or even an air-conditioning vent. Since these cannot be detected by electronic sweeps, finding them involves carefully X-raying every square inch of a building or tearing apart the walls.

Some eavesdropping methods dispense with bugs altogether. Computers give off radio waves that can be picked up by interception equipment outside a building—in a van parked as far away as a mile, perhaps—and then translated by another computer. In theory at least, words typed on a computer screen will appear almost simultaneously on a second screen in the van. Experts differ on how close this technique is to being usable. One figures that a skilled technician could put the basic interception equipment together from components that can be bought in any electronics store for about $300. Maybe so, counters Frank Mason, president of a Fairfield, Conn., company that makes countermeasure devices for the Government, but "you would need almost laboratory equipment" to get a good reproduction. Protecting computers against such snooping is expensive. Metal shields can be placed around computers to contain the electronic pulses, but one expert estimates that installing and inspecting the shielding would cost more than $200,000 for each machine.

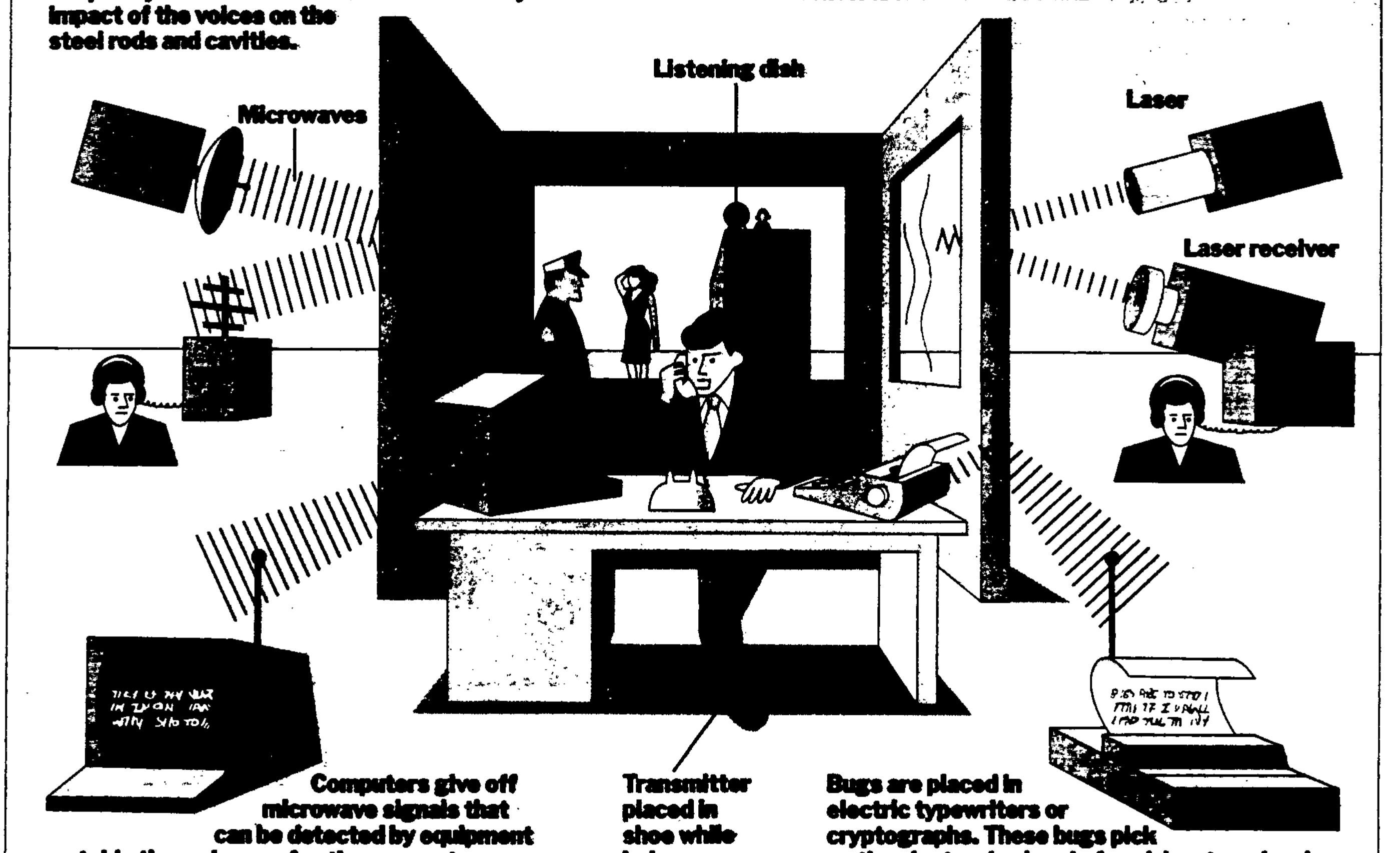
The most exotic technique of all is to play laser beams against a window or any surface that vibrates slightly with sound waves. The laser beam senses the minute reverberations and transmits them to a computer that converts them back into sound. Richard Heffernan, vice president of Information Security Associates, a Connecticut firm that makes countersnooping equipment, doubts that this technique is all that practical—yet. A window, he explains, vibrates not only from voices inside but also with sounds that strike it from outside: jets overhead, traffic below, birds chirping. "Picking something off the window is difficult to do in most locations due to the high ambient noise outside," says he. Another expert, however, says the Defense Department is concerned enough about laser snooping so that it has rigged the walls of rooms in the Pentagon where sensitive conversations are held to continuously give off white noise—vibrations that might confuse the laser beams. So far as is known, this countermeasure has not been used in the Moscow embassy.

For a long time American experts have worried about mysterious low-level microwaves that have apparently been beamed at the embassy building. One explanation involves a possible type of snooping that does not require hidden transmitters in the building. Mysterious cavities along with configurations of steel rods and wire mesh have been found in the walls of the new embassy complex. It

STATE-OF-THE-ART SURVEILLANCE

Listening devices can be built into the walls of the embassy. An arrangement of steel reinforcing rods or cone-shaped cavities is hidden in the walls. Microwaves are beamed at the walls, and a computerized receiver differentiates how the frequency of the microwaves is modulated by the impact of the voices on the steel rods and cavities.

Sound and words cause windows in the room to vibrate. A laser beam is directed at the window. The beam is reflected and picks up the vibrations of the window. A computer then reads the beam and converts it back into sound.



Computers give off microwave signals that can be detected by equipment outside the embassy. Another computer analyzes the signals and recreates the original information.

Transmitter placed in shoe while being repaired

Bugs are placed in electric typewriters or cryptographs. These bugs pick up the electronic signal of each key typed and transmit it to antennas hidden in the embassy wall. The antennas relay the signal to a listening post outside.

TIME Diagram by Joe Lertola

Continued

is theoretically possible that the microwaves could somehow pick up the reverberations that emanate from within the walls of a building; a computer would then analyze those reverberations.

Diplomats who have served in Moscow insist that Americans have assumed for decades that all their conversations might be overheard, and made it a rule to take precautions. George Kennan remembers discovering a Soviet bug in the Ambassador's residence when he was a young foreign-service officer in Moscow in the 1930s and finding a more sophisticated one in the beak of the eagle in the Great Seal of the U.S. when he was Ambassador to Moscow in 1952. (President Eisenhower disclosed that bug years later during the U-2 spyplane crisis.) Says Kennan: "For half a century at least we've gone on the theory that the premises we occupied in Moscow were not safe unless special precautions were taken."

One precaution was the "bubble," a supposedly bugproof, heavily shielded room-within-a-room in the embassy. But now it is assumed that Marine guards let Soviet agents into the bubble to plant bugs there too (two new bubbles have since been built). The greatest damage would have been wrought if a bug in the encoding equipment did indeed allow the Soviets to crack the U.S. code and read all messages going into and out of the embassy. Presumably these would have included U.S. negotiating positions. Says John Barron, author of a book about the KGB: "Give me access to your ciphers, and you won't have any secrets."

There is hot disagreement over whether any part of the new U.S. embassy can ever be made safe for anything except the most mundane conversations. No one seems to think that all the bugs in the building will ever be found. To do so might require conducting what one expert calls a "destructive search"—which means nothing less than tearing the building apart. But some optimists believe that at least some rooms can be made secure, mostly by shielding them in copper, lead or other materials that foil electromagnetic emissions.

But there is a strong current of opinion among specialists that the whole building is hopeless and the only thing to do is raze it and start over again with materials prefabricated in the U.S. "Putting up the building has just got to be a bugger's dream," says one expert. Hal Lipset, a San Francisco private investigator who won fame in the 1960s by concealing a bug in a martini olive, agrees: "The whole building is one big microphone." If that advice is followed, however, the U.S. for many years would have to keep conducting diplomacy in the old building, which has apparently been sown with sophisticated bugs that have so far proved impossible to find. ***—By George J. Church. Reported by Jay Peterzell/Washington and Raji Samghabadi/New York, with other bureaus***