ARTICLE APPEARED ON PAGE 1-12

LOS ANGELES TIMES
13 April 1987

Sophisticated New Devices

KGB Eavesdropping Pervasive, Persistent

By ROBERT GILLETTE, *Times Staff Writer*

WASHINGTON—It was one of the more dramatic moments in the modern history of electronic counterespionage. U.S. Ambassador to Moscow George F. Kennan sat in the study of his ornate residence in 1952 and read aloud what he hoped the KGB, listening through a device suspected of being hidden somewhere in the room, would believe was an authentic message to Washington.

As Kennan read, two technicians scurried about with their detection instruments, homing in on a radio bug like excited hounds on the scent. Suddenly one snatched a wooden replica of the Great Seal of the United States from the wall and smashed it open.

"Quivering with excitement," Kennan recalled in his memoirs, "the technician extracted from the shattered depths of the seal a small device, not much larger than a pencil." With the discovery of this "fantastically advanced bit of applied electronics," he wrote, "the whole art of intergovernmental eavesdropping was raised to a new technological level."

In the intervening 35 years, nothing has changed and everything has changed.

As the current furor over espionage and bugging in the U.S. Embassy in Moscow makes clear, the KGB's determination to penetrate its primary target in the Soviet capital remains as high as ever.

What is new, in the view of some U.S. officials investigating security breaches at the existing embassy and the unfinished $190-million American compound immediately behind it, is the multiplicity of techniques that recent advances in microelectronics have made possible.

The amazing device uncovered in Kennan's office 35 years ago seems hopelessly primitive today. Bugs themselves have shrunk to inconspicuous motes the size of rice grains, and microwave beams, lasers, fiber-optic technology and computers have joined the armamentarium of high-technology snooping. Among the discoveries of the last decade:

—A sophisticated antenna capable of being raised and lowered through a disused chimney in the U.S. Embassy in Moscow

Devices in Typewriters

—Tiny devices implanted in the embassy's electric typewriters that could read messages before they were encoded and transmitted.

—The suspected connection of the structural steel of the new U.S. Embassy, which is still in construction, into a huge radio antenna that can broadcast information detected by bugging devices hidden inside the building.

The Soviets have no monopoly on spying. In Moscow last week, the Kremlin displayed a wealth of electronic listening devices it said it had found in Soviet offices and homes in Washington, New York and San Francisco.

But one U.S. official familiar with the current investigation of U.S. security lapses in Moscow said the "Soviets are very, very competent—in some ways, years ahead of us" in the technology of eavesdropping.

A Standing Assumption

Since the end of World War II, "hundreds, if not thousands, of microphones have been concealed inside American installations," Harry Rositzke, a retired Soviet specialist with the CIA, noted in a 1981 book on the KGB.

According to diplomats who have served recently in the Moscow embassy, it is a standing assumption that the Soviets can monitor conversations in ordinary offices of the building, which the Soviets originally constructed as an elite apartment complex and turned over to the United States as an embassy in 1952.

One low-tech countermeasure, diplomats said, is to scribble the sensitive parts of conversations, such as the names of Soviet contacts, on a yellow legal pad. At home, many foreigners use a child's "magic slate" for the same purpose.

Important conversations and conferences are conducted in specially designed "secure rooms." They are described in published reports as rooms within rooms, shielded to prevent the penetration or escape of all sound and electromagnetic energy such as radio signals or microwaves.

"Properly constructed and properly inspected, these rooms are 100% secure," an experienced government security officer said in an interview. "There are certain physical laws that even the Soviets can't violate."

Ronald I. Spires, undersecretary of state for management, said it is "generally true" that devices using microwaves can overhear conversations in almost any unprotected room. "In those kinds of environments, nobody in his right mind would conduct a conversation he doesn't want overheard," Spires said.

Two Marine guards have been accused of letting Soviet agents enter the most secure areas of the embassy in 1985 and 1986 and a third has been detained on suspicion of espionage during his posting at the American Consulate in Leningrad in 1981.

Arthur A. Hartman, who retired as U.S. ambassador to Moscow in February, was conscious of Soviet bugging and sought to turn it to good advantage, said a senior diplomat with long experience in Moscow.

"He *wanted* the Soviets to hear 95% of what he had to say—when he briefed a congressman, for example," the diplomat said. "This was one way he had of getting his ideas across to the Soviets. For the other 5%, you had the secure rooms."

However, he and others noted that lower-ranking embassy staff could not always be counted on to distinguish as clearly between what could and could not be said outside secure areas.

Outside the embassy walls, the bugging of foreign apartments is considered so pervasive and the equipment so easily replaced that U.S. officials do not even bother "sweeping" the living quarters for Soviet bugs.

Continued

"It would only make them mad, and they might steal something in retaliation," noted one diplomat who served in Moscow. Debugging diplomatic apartments, he added, would also encourage a false sense of security.

Debugging Is Hopeless

Soviet agents, seemingly to intimidate foreigners and remind them that debugging is hopeless, occasionally leave telltale signs of their regular visits to foreigners' apartments—a roll of film stolen from a personal camera tucked away in dresser drawer, a toilet used and left unflushed, a piece of trash left on the floor.

Several years ago, one West European military attache who lived alone in Moscow discreetly attached a counting device to his front door and found that the number of openings and closings was roughly twice what his own comings and goings could explain.

"Talking to the walls" has become a time-honored technique among foreigners for demanding repairs and other services from the notoriously uncooperative government service agency.

The wife of a former security officer at the American Embassy, for instance, recalls complaining long and distinctly to her kitchen walls several years ago about the disappearance of her favorite butcher knife, seemingly purloined by the Soviet maid. She came home from work a few days later to find a lump under the living room rug. It was the knife.

Although microphones buried in the walls may still serve their purpose, the KGB and its allied security agencies in Eastern Europe now have much more sophisticated and convenient devices, according to diplomatic sources.

One, these sources said, resembles an inconspicuous bit of copper wire that can be installed in moments behind the wall plates of electrical outlets. The device resonates to the sound of voices and transmits its signals through the building wiring.

U.S. diplomats are warned that conversations are no safer outdoors than indoors. According to a former senior diplomat at the American Embassy, the technology of directional microphones has advanced so far that "you cannot go outdoors and conduct a conversation safely anywhere in the Soviet Union."

Among ordinary Russians, it is widely accepted that the KGB is capable of selectively monitoring conversations in any apartment by listening through the telephone, even with the receiver on the hook. According to a dissident electronics engineer in Moscow, one technique is to transmit through the receiver an ultrasonic tone—inaudible to human ears—that is modulated by voices in the room. The mouthpiece then returns the modulated signal, which is processed to extract the voice component.

Image of Omniscience

While the KGB may circulate such tales to promote an image of omniscience, many Russians take it seriously enough to disconnect their telephones or bury them in pillows when friends visit.

The KGB, probably like other intelligence agencies, appears to reserve its most sophisticated and ingenious bugging technology for its potentially most productive targets. Foremost in Moscow is the U.S. Embassy.

Although U.S. authorities are reluctant to describe Soviet systems found at the embassy, it is clear that countersurveillance experts have uncovered at least three major technological surprises in the last 10 years.

In 1978, security officers found a sophisticated transmitting and receiving antenna in a disused chimney of a residential wing. The antenna, capable of being raised and lowered, evidently to scan various floors of the 10-story embassy, was connected to cables that led through a previously undiscovered tunnel beneath the building. points outside the building.

In the spring of 1983, the United States used neutron radiography equipment that, in effect, X-rayed The tunnel led to a nearby apartment building.

U.S. officials said at the time that the antenna appeared to represent a unique variety of eavesdropping technology. Some published reports have said the antenna may have been designed to pick up emissions from bugged typewriters, while other reports suggest that it was intended to activate listening systems that lay dormant—and thus harder to detect—until needed.

Even now, officials refuse to specify the purpose of the antenna. "It took us a while to figure out what they were doing," one said.

A second major revelation was the discovery in 1984 of ingenious microelectronic devices implanted in a number of the embassy's electric typewriters. Each press of a key transmitted a distinctive signal down the typewriter's power cable and into the building wiring. Computers could then reconstruct the cables exactly as they were typed. In this way, officials familiar with the technology said, the Soviets were able to intercept cables before they were coded, circumventing an encryption system that is considered unbreakable.

Wholesale Bugging

Officials said the bugs were probably installed when the typewriters were shipped from Western Europe to Moscow. One source said they were briefly in the hands of a Western European shipping firm in which the Soviet Union had a controlling interest.

The greatest problem faced by the Americans is the wholesale bugging of the eight-story office building that is part of their $190-million embassy complex under construction immediately behind the present embassy. Under a 1972 construction agreement, the Soviets were allowed both to design the major structural elements of the complex and to fabricate them away from the site, providing extensive opportunity to rig the building for eavesdropping.

Spires, the undersecretary of state, said that in retrospect it was "beyond belief" that the Nixon Administration gave the Soviets such latitude.

One official familiar with the current investigation explained: "The Soviets would never have agreed to any conditions that would prevent them from bugging the place. They don't do things that are not in their interest."

According to other government sources, the problem is not simply that sophisticated devices have been planted in the building but that, in a sense, the building itself is a bug. Soviet engineers, they said, appear to have incorporated cavities in prefabricated structures to conduct sounds or to carry fiber-optic threads to convenient pickup the walls and floors of the building. Accounts differ about what was found. But according to one official, the radiography "essentially confirmed" that the building had been wired for sound.

In addition, some analysts believe that steel girders and reinforcing rods embedded in the concrete walls have been deliberately arranged to provide surreptitious pathways for electronic signals. It is feared that the steel structural elements of the building may function as a huge radio antenna, to broadcast information that bugging devices pick up.

The State Department has asked

Continued

former Defense Secretary and CIA Director James R. Schlesinger to recommend whether the building should be torn down. Several officials familiar with Schlesinger's study said there were persuasive reasons for not razing it.

"With a certain amount of time and money, you can pretty well neutralize what the Soviets have done," a veteran security officer insisted. "No building can be made 100% secure—that's why you have secure rooms."

And a State Department official pointed out: "Now, you're dealing with 1977 [bugging] technology. Rebuild it, and you're going to have to deal with 1987 technology."

Staff writers Norman Kempster and Robert C. Toth contributed to this story.