# Evading the Soviet Ear at Glen Cove

*The government, opposed to the deportation of spies, wages a quiet war against electronic ears at Soviet missions*

The city of Glen Cove on Long Island decided to boot Soviet personnel off beaches and tennis courts when the media reported that a diplomatic residence outside town was a center for electronic espionage.

On Capitol Hill, a more recent response has been a drive to kick spies out of the country. Representative John LeBoutillier (R–N.Y.) introduced a bill on 18 August that calls for deportation of diplomats who the President "has reason to believe" are engaged in electronic surveillance. The bill is identical to one recently reintroduced by Senator Daniel P. Moynihan (D–N.Y.), who has complained of Soviet snooping for years.

In spite of growing momentum, attacks on the spies are unwise, according to a variety of government officials. For one thing, the Administration fears response in kind. Moreover, a ban on electronic espionage would mandate a virtual exodus of "diplomatic" personnel from the United States. "Just look out over the roofs of Washington," says an official in the telecommunications industry. "There's a lot going on that's somewhat less than legitimate." Finally, the government knows the whereabouts of eavesdroppers. If spies were forced underground, efforts at monitoring would be impossible.

In lieu of deportation, the government has waged a quiet war against the practioners of electronic espionage for the past 5 years. It has tried, with more cloak than dagger, to protect telephone links from the onslaught of sophisticated gadgetry. The problem looms larger each year.

What originally upset the people of Glen Cove was the disclosure in April by a top Soviet defector that the 36-acre Killenworth estate was not just a fancy retreat for Soviet personnel at the United Nations but a nerve center for electronic espionage. The disclosure was made by Arkady N. Shevchenko, who in 1978 resigned as Under Secretary General to the United Nations and took up residence in the United States—the highest ranking Soviet official ever to defect. In an interview on *The KGB Connection*, a Canadian-produced TV documentary, Shevchenko blithely described what went on in the 49-room mansion: "All the top floors of the building are full of the sophisticated equipment for the, ah, to intercept all the conversations, telephone conversations on anything which is going on," he said with a grin. "At least 15 or 17 technicians were working to do all this job."

The revelation touched off a spate of reprisals, cold war rhetoric, and diplomatic maneuvers. It also shed light on capabilities quietly enjoyed by the Soviets for years. Says Alan M. Parente, mayor of Glen Cove: "To the best of my knowledge, they can sweep in signals from all of the Northeast corridor—New Jersey, New York, Connecticut, Long Island, maybe even Massachusetts."

Communication experts agree, saying telephones can be tapped at a distance of 100 miles. This would put the Navy's submarine base at Groton, Connecticut, within easy reach of the Soviet ear at Glen Cove.

> "They can sweep in signals from all of the Northeast corridor."

What makes telephones so vulnerable to clandestine connection is the explosive growth of microwave communication links during the past 30 years. Microwaves first sped messages from coast to coast in 1951, moving calls in 30-mile hops from one relay tower to another. The system proved much cheaper than buried wire cables. By 1960, microwave relays provided the Bell System with more than a third of its connections between cities. Today the vast majority of long-distance calls are transported via microwave, each link in the nationwide chain carrying about 2000 conversations.

Microwave is often likened to a powerful flashlight—a concentrated beam of high-frequency energy that flashes from relay to relay. Popular wisdom holds that a spy must place an antenna along the beam path in order to capture a signal. Not so, say experts in government, industry, and academia. Much of the energy may be concentrated into a tight beam that spreads little between relays. Yet a microwave transmitter also puts out weak signals that radiate in all directions.

For spies, microwave is more like a beacon. A clandestine ear, moreover, with high-gain antennas and low-noise amplifiers, can monitor signals over vast distances. The most dramatic example is the U.S. satellites that for years snooped on microwave signals in the Soviet Union, capturing, among other things, highly classified data transmitted during missile tests. Known as Rhyolite, this type of satellite spied from geosynchronous orbit—23,000 miles above the earth.

Tapping a U.S. microwave beam would still be a tough job except for two things. First, the telephone company conveniently encodes the dialed number right before a call. This identifier allows a selective search among the 2000 calls on a microwave beam, say, for 202-456-0000, the general format of long-distance calls to the White House. Second, high-speed computers make the search automatic, freeing a spy for other tasks. "They don't have to have a million people listening in," says Martin E. Hellman, an electrical engineer at Stanford University. "They just have a computer that scans across the dialing tones and activates a recorder when something interesting comes across."

What all this adds up to is a vast power to spy with impunity—a disconcerting fact that dawned on the government rather slowly. "In the early 1970's, the Soviets could monitor all the telephone calls to and from the Department of Agriculture, and they ended up knowing more about the American grain market than we did," says Harry Rositzke, a 25-year-veteran of the CIA. "That's how they got that great grain deal."

The Ford Administration was the first to grapple with the problem. By 1977, Jimmy Carter signed Presidential Directive 24, a top secret document that called not only for increased care in the transmission of classified data and conversations but also for the Commerce Department to take the lead in protecting "sensitive" U.S. information, such as com-


0036-8075/82/0903-0910$01.00/0 

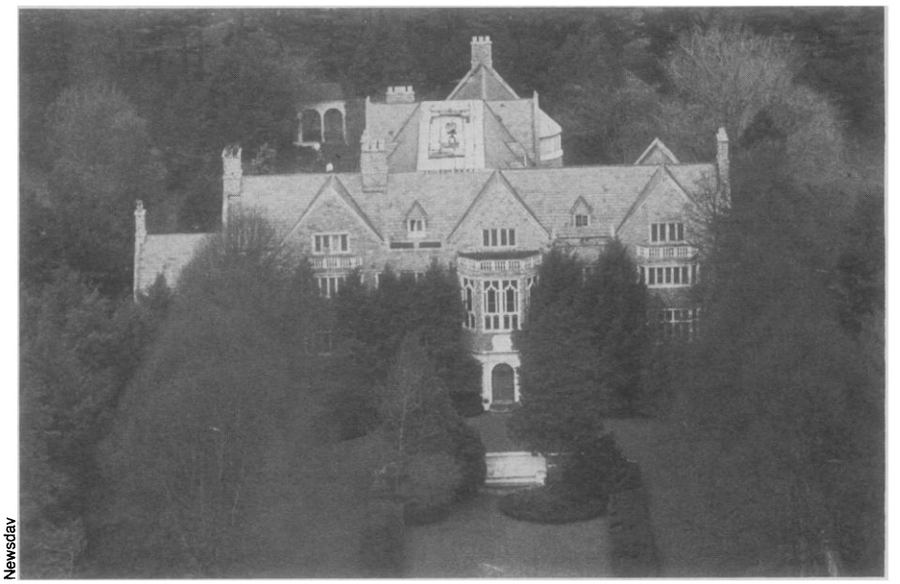
modity market forecasts (especially the availability of critical materials), financial data (changes in the prime rate or support of the dollar in foreign exchange markets), the status of oil reserves, and so forth. In 1978 an antispy unit at the Department of Commerce, known as the Special Projects Office, started advising U.S. agencies on how to prevent electronic theft.

The easiest solution is to route government phone conversations through underground cables, but short supply makes this possible for relatively few calls. Therefore the Carter program expanded the government's Executive Secure Voice Network, which uses scramblers to jumble messages beamed over microwave. Even more resistant to eavesdropping are encrypted calls, where messages are taken apart according to an exact code rather than just rearranged. Yet encryption is not possible across a whole network since most microwave transmissions are analog rather than digital and cannot be encrypted on a wholesale basis. An expensive solution (up to $20,000) used by some government agencies is a machine known as a personal encrypter, which both digitizes and encrypts but has the unfortunate side effect of reducing voice quality. To help federal agencies pick through the welter of scramblers and encrypters, the Special Projects Office in 1981 put out a 154-page book that identifies 32 vendors marketing 160 different devices to outwit electronic spies.

Relatively few federal calls can be protected, even though the vast majority can quickly, sometimes accidently, become "sensitive." Some agencies thus keep tabs on employees.

"This is a nonsecure telephone subject to communications security monitoring," reads a red label on a Navy phone at the Groton sub base. "Use of this phone constitutes consent to monitor." The Navy sometimes listens to see if vital data might be slipping into the hands of the Soviets.

A more graceful way of thwarting spies is to make microwave networks less amenable to penetration, something the government has tried to do within the past year. Previously, the Federal Communications Commission gave out the coordinates, frequency, and power output of microwave transmitters to anyone who asked. The aim was to help contractors setting up new microwave networks to avoid routes and frequencies that were already chaotic from overuse. Yet it was also a virtual how-to guide for aspiring spies. Today, contractors who want data on government-used microwave links must put in written requests to the National Telecommunications and Information Administration. Requests are often denied.



Newsday

***Killenworth: Listening in on the defense industries of Long Island***

*"All the top floors of the building are full of sophisticated equipment."*

The biggest hurdle to electronic espionage is yet to come—the removal of the code that advertises where a call is destined. The telephone industry is putting calls and destination codes on separate microwave paths. Known as Common Channel Interoffice Signaling, the technique by 1985 will add a measure of protection to about 65 percent of all long-distance calls. A spy will eventually be forced to monitor millions of calls to determine if a conversation is worth recording. Alternatively, a computer could listen for "key" words, although such techniques presently allow the reliable recognition of only about 100 words.

For the moment, government officials admit protection is spotty. The most important calls are impervious to capture, but the vast majority are protected partially if at all. The problem is compounded because of the vast amount of classified and "sensitive" work done outside the government.

The listening post at Glen Cove can pick up calls across the length of Long Island and thus monitor all of the island's defense industries. For the most part, Long Island companies do not seem alarmed. Defense firms say they have standing rules forbidding discussion of classified information on the telephone and that security systems are regularly monitored by the federal government. However, security may be somewhat less than ideal, as indicated by a spokesman for Grumman Aerospace who told a reporter that microwave interception was impossible because the Soviet residence at Glen Cove was not exactly midway between two Grumman test facilities.

To help local industry cope with Soviet snoopers, Representative LeBoutillier has been calling officials at Fairchild, Grumman, Eaton, Sperry Rand, and other Long Island defense industries, encouraging them to tighten up security and to realistically grapple with the threat of electronic espionage. LeBoutillier says the recent bill is more an expression of congressional sentiment than a plan for deportation.

The quiet war against the eavesdroppers needs all the help it can get. An emerging problem is the proliferation of communication satellites, which beam myriad calls over large areas—a few thousand miles from side to side. Anyone with a dish antenna and a bit of equipment can monitor the microwave signals. The Soviets are said to intercept transatlantic calls at a sophisticated earth station in Cuba. In the meantime, life goes on as usual at the Soviet estate of Killenworth, situated atop a small hill that gives a panoramic view of the Long Island countryside. Probably not the least interesting work is the monitoring of "microwave alley," the name U.S. experts have for Long Island Sound. It is so named because microwaves travel best over water. Says an industry official: "The [Soviet] property is ideally located." Just across the Sound, 12 miles north of Killenworth, is a microwave relay tower at Stamford, Connecticut. It relays signals up and down the eastern seaboard for the New York Telephone Company.—WILLIAM J. BROAD