ARTICLE APPEARED
ON PAGE 40

U.S. NEWS & WORLD REPORT
8 April 1985

Pulling the Plug on Soviet Eavesdroppers

Electronic spies will get an earful of gobbledygook rather than vital secrets once a new U.S. plan is implemented.

A Pentagon consultant telephones a defense contractor, asking about a new missile's supersecret guidance system.

Across town, one of a half-dozen antennas bristling atop the Soviet Embassy intercepts the call and feeds the signal into a computer. Sensing a familiar dial-tone sequence, the computer records the conversation for analysis.

The incident is hypothetical. But U.S. officials say real episodes of this kind happen daily as the Soviets expand an already impressive capacity to carry out a wide range of esoteric snooping.

Now, the Reagan administration is fighting back. A plan was announced on March 26 to develop a better type of secure phone that would foil Soviet electronic spies. The aim is to install hundreds of thousands of these phones in offices of government security agencies and defense contractors.

Typewriters bugged. The decision reflects widespread concern in Washington over a possible hemorrhage of secrets to Moscow. "The Soviet Union is making major efforts to intercept and walk away with our secrets," asserts Donald Latham, the Pentagon's communications-security chief.

Latest example: It was confirmed in late March that the Soviets had placed tiny transmitters in typewriters shipped to the American Embassy in Moscow. Sensors hidden in the embassy's walls apparently picked up the tapping of keys being struck, thus revealing to the Kremlin what was written.

Often, there is no need to plant a bug or tap a phone line. Huge volumes of secret information simply go through the air, free for the taking.

Soon, the Soviets may have an even better listening post in Washington.

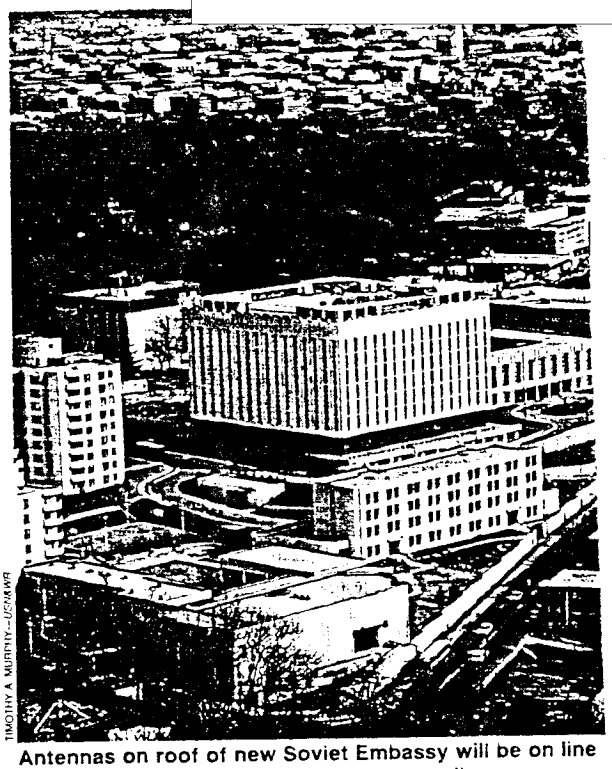
Moscow's new embassy, now nearing completion, sits atop a 350-foot hill with a clear line of sight to the White House, the Pentagon and commercial communications towers. Antennas there will be able to pick up any messages sent through the airwaves.

Giant antennas in Cuba permit the Soviets to listen in on most messages carried by satellite from one point to another in the U.S. and even to pick up some international messages carried by the Intelsat network.

Other communications are simply plucked from the air by banks of antennas at the present Soviet Embassy in Washington and posts in New York and San Francisco.

Scooped up wholesale from the ether, these messages are run through computers programed to recognize certain phone numbers and names. If the message is sent by machine, such as a telex, the computer prints it out.

If the intercept is a telephone conversation, it must be transcribed and translated. Moscow is said to have assigned thousands to this task.



TIMOTHY A. MURPHY—USN&WR

Antennas on roof of new Soviet Embassy will be on line of sight to intercept secret Washington calls.

All major defense contractors have at least one secure phone. But, for a busy manager or engineer, it is always easier to pick up the insecure phone a few inches away. "People are way too careless with their use of phones," Latham says.

They are also careless with facsimile machines that send drawings and other documents over phone circuits. "The tendency is to say, 'This is sensitive, so I'll send it by fax.' That's just giving it to them in writing," says J. Michael Nye, president of Marketing Consultants International, a Maryland communications-security firm.

Officials are reluctant to cite instances of secrets purloined in this way. But the interception and decoding of enemy communications in wartime has been demonstrated on many occasions. Most recently, the North Vietnamese made use of intercepted messages to warn their troops of U.S. attacks.

Yet it was not until the late '70s that officials fully awoke to the fact that hostile intelligence agencies were able to listen in as government officials and defense contractors chatted over unsecured phones in this country.

The Carter administration reacted by connecting key offices in Washington and several other cities with underground wires rather than relying on microwaves, which travel through the atmosphere from one point to another.

The government also equipped a few offices with phones that scramble and unscramble conversations. But these instruments, still in use, cost $9,000 or more apiece, are awkward to handle and produce distorted sounds. And the vast majority of government communications still take place over ordinary phones.

In Washington's new drive against electronic spying, the National Security Agency announced on March 26 that three companies—RCA, AT&T and Motorola—would share a 44-million-dollar grant to develop improved scrambler phones. The government expects to buy half a million of them for less than $2,000 apiece.

Tiny coded key. The new phones, when they come into use in 1987, will be easy to use and will sound like an ordinary phone. A coding device about the size of a pack of gum is inserted in the phone while it is in use and can be locked away in a safe at other times. Even for top-secret security, the coded key will only have to be changed once a year.

When a call is made, one phone queries the other and tells the user—with a light or electronic-display panel—what level of security is being provided.

"Our goal is to put one of these on every guy's desk," says Latham.

Once production lines are running full speed, the secure phones will go into other government offices and be sold to financial institutions and other firms whose messages, while not classified as secret, are still sensitive.

No one thinks the secure phones, by themselves, will prevent a determined foe from trying to listen in. But it will no longer be the free ride that it is today. □

By ORR KELLY