25 JUL 1977

The unsettling growth of spying by microwave

est Volkman
Service

ive years ago, a small of Army electronics intelli- experts set up shop in the nt of the U. S. Embassy in . In the process, they opened chapter in the espionage war n the United States and the Union that has led to a contro- over whether U. S. domestic ications themselves are se- om outside snooping.

-named USM-2, the unit's ac- were so secret that only a few can officials were aware of it was doing. Basically, its n was to utilize the newly de- d art of intercepting communi- signals, including telephone sent by microwave transmit- Around the clock, the Ameri- who were on loan to the Na- Security Agency, beamed their oring devices all over Moscow, to pick up top-secret trans- ons by Kremlin leaders.

early 1972, USM-2 struck pay By chance, American intelli- had discovered that the Krem- aders, as they rode to their of- in limousines, would discuss sensitive matters over radio hones in the cars, a communi- system the Soviets considered secure from eavesdropping. But the Americans, beaming their monitors from the embassy, heard every word, intelligence that proved so valuable that it was sent directly to the White House under the code name VIPAR.

As with most such operations, it was only a matter of time before the Soviets figured out what was happening. And they reacted strongly, beaming heavy doses of radiation with microwave transmitters into the American Embassy to jam the monitoring devices. The beaming, which led to outbreaks of illness among U. S. diplomatic personnel, was finally scaled down last year after strong protests by the White House.

The episode, some details of which were later revealed in congressional testimony, gave the public a rare peek for the first time into the new frontier of espionage. That frontier involves the interception of a growing amount of communications that are sent via microwaves, ultra-high frequency radio waves that can handle a large amount of data in a narrow spectrum. In the process, a new problem has surfaced — how can the communications by microwave be protected?

The question is at the heart of a current debate within the Carter Administration over a proposal by the National Security Agency (NSA) that the United States set up a complex series of controls to safeguard U. S. microwave communicatons. NSA officials argue that the Soviets have been increasing their monitoring of U. S. transmissions (an increase that some experts believe was in retaliation for the U. S. program in Moscow) and there is an urgent need to safeguard them.

The NSA argument underscores the amazing growth of microwave technology in the past decade. Currently, nearly 60 percent of all U.S. domestic long-distance calls are sent by microwave transmission. Additionally, federal agencies and private businesses each day transmit literally millions of pieces of data over facsimile machines, teletypes, Telex service and other printer traffic via phone lines that use microwave transmission.

But the technology is a mixed blessing to intelligence agencies, because not only are microwave transmissions sent into the open air easy to intercept, but each transmission contains a large amount of data. The task is made even easier by computers. The NSA, which has nearly 2,000 monitoring posts around the world, collects so-called "raw" transmissions, tapes them, then feeds them into huge computers that are programmed to pinpoint data of particular interest. The Soviet interception effort, while not as good as the U.S. effort at the moment, is growing.

The problem of protecting microwave transmissions in general is difficult, since microwave technology is growing faster than the technology to make them secure from snooping. At the moment, there are two main ways to do it. One is to "scramble" voice transmissions to make them sound, as one expert phrased it, "like Donald Duck speaking Chinese." An "unscrambler" at the other end of the conversation makes it intelligible again.

The second method is to encode the transmissions at the microwave relay point, decoding the conversation at the other end.

The problem with both methods is that they are expensive; nobody knows exactly how much, but some estimates run into the billions.

The task of intercepting such data, on the other hand, is considerably simpler and cheaper. As a Senate investigator of U.S. intelligence agencies noted last year, "Any individual with an instruction manual and a few thousand dollars worth of equipment can ... record continuously calls on