Seized Ship Part of Worldwide Intelligence Net

24 JAN 68

By EVERT CLARK
Special to The New York Times

WASHINGTON, Jan. 23—The intelligence ship Pueblo was one unit in a vast network of electronic eavesdropping devices that the United States operates on land and sea, in the air and in space.

Engineers who have seen Defense Department photographs of the ship have no doubt that it was trying to pinpoint the sites of key radio and radar stations in North Korea, one of the world's most likely trouble spots.

There is some feeling here that the Pueblo was trying to take down on magnetic tape the electronic signatures of Soviet-built antiaircraft and missile-guidance radars.

Such signatures are needed so that American engineers can design jamming devices and other electronic countermeasures to cripple a radar in the event of combat.

Electronic warfare, according to the experts, has emerged in Vietnam as a necessity for victory in modern war.

Pilots Rely on Devices

The magazine Aviation Week & Space Technology noted this month, in a study of electronic warfare in Vietnam, that "few pilots now wish to fly without ECM (Electronic counter measures) equipment, although it sometimes must be carried at the expense of extra fule tanks or payload."

One report today said that the Defense Department had identified the Pueblo as an environmental-research ship. In a technically complex world where radio, radar and satellite communications play a vital role in warfare, "environment" often mean the electronic surroundings, rather than more tangible phenomena.

Vessels Seek Electronic Data on Missile-Guidance Radar Designed by Russians

The vessel was also described as a modified auxiliary light-cargo ship, and—perhaps more pertinent—a Navy intelligence-collection auxiliary ship.

The 179-foot Pueblo is much smaller than the Liberty, a similar American spy ship that was heavily damaged by the Israelis in the Mediterranean last summer with the loss of many lives.

But the liberty and the Pueblo are typical of ships, submarines, planes, unmanned drone aircraft and satellites used to listen and to learn everything possible about the energy emitted by the enemy's electronic devices.

As Old As Radio

Eavesdropping on an enemy radio messages is an old as radio itself. The aim is usually to find out the content of the transmission, rather than to determine the frequency or to learn what kind of equipment is being used.

Eavesdropping on enemy radar has a different purpose, since radar is used not to carry messages but to find a hostile ship, plane, missile or satellite and sometimes to direct a counterweapon toward it.

To listen furtively to an enemy radio and find out what military messages it carries takes time, so a ship that can stay on station or cruise in a limited area is an ideal vehicle.

To ferret out new radar frequencies takes less time, but it is a more complex task and often very risky.

Each side must know the location and radar signature of the enemy's radar to put it out of commission with bombs or missiles or to confuse it with spurious radio beams or physical targets. Small pieces of aluminum "chaff" were first used for this purpose in World War II and are now considered a primary "spoofing" weapon against antiballistic missiles.

The Soviet Union and the United States have each used a "feinting" technique to make the other side beam radar on an aircraft and thus reveal its frequencies. American aircraft have penetrated close to Siberian defenses, for example, and Soviet planes have pushed near the Distant Early Warning line in Canada. This may force the other side to turn on the radar that would be used in wartime, just in case there is a "peacetime" frequency, with a more efficient frequency used only in wartime.