ARTICLE APPEARED ON PAGE 1

BOSTON GLOBE
5 June 1986

Pelton's 'top-secret' intelligence not so secret

US claims security compromised, but many key details in public domain

By Fred Kaplan and Walter V. Robinson
Globe Staff

WASHINGTON – In a crowded federal courtroom in Baltimore, only carefully selected, elliptical references have been made to the top-secret communications intelligence Ronald W. Pelton is accused of selling to the Soviet Union for a paltry $35,000 in cash.

R. W. PELTON
Accused spy

Thirty-seven miles away in the nation's capital, top US intelligence officials have emerged from the silence that shrouds their agencies in secrecy to threaten reporters with prosecution for publishing articles about the intelligence that can be assembled, for the most part, from unclassified technical manuals, pre-trial statements in open court and even from past news reports.

In the two cities, the government appears to be making contradictory arguments: Prosecutors in Baltimore have asserted that Pelton sold a treasure trove of intelligence data to the Soviets that destroyed a successful intelligence program. But officials in Washington have warned that even general press speculation about the program may alert the Soviets to things they do not know.

Obscured under this extraordinary security blanket, according to sources, is the program the Soviet Union is undoubtedly aware of because of the information it gleaned from Pelton, but one which could prove embarrassing to the United States if it were to become publicly known.

According to the sources, the program involved the use of US Navy submarines, creeping into Soviet waters at great risk, to facilitate eavesdropping on an undersea communications system – an underwater replay of the U2 overflights of the Soviet Union that became a deep embarrassment to the United States in 1960 when one of the reconnaissance planes was shot down and its pilot, Francis Gary Powers, was captured.

With the help of a high technology device, identified by Pelton in trial testimony this week as a "recording system," US satellites orbiting in space were privy to top-secret Soviet communications.

The US operation that was compromised, code-named "Ivy Bells," allowed the United States to intercept messages that Soviet submarines sent to military command posts ashore when they returned to their harbors after sea cruises. Among other things, the messages included information about where the Soviet subs had been and what they had done.

Before Pelton compromised the program, it had been an intelligence coup that apparently enhanced the hegemony of US submarines over Soviet subs in the grim undersea cat-and-mouse game that has a major role in the superpower struggle for nuclear superiority.

Eleven years after some US intelligence officials rebelled publicly against a predecessor program, arguing that the use of US submarines in Soviet waters was too dangerous and had no place in an era of superpower detente, the issue has surfaced anew, although only obliquely this time.

Some details omitted

Senior US intelligence officials have insisted, in meetings with Globe reporters during the last week, that publication of information about the programs compromised by Pelton could severely damage US national security.

Although these officials have repeatedly declined to provide specific information to support such claims, The Globe has omitted from this article a number of important technical details about the program, and has described others only in general terms.

Under the ground rules governing the meetings with the officials, the Globe cannot publish the general arguments they raised about why publication of the information could damage US national security.

Because of such government sensitivity, the trial has also produced only limited mention of another program Pelton allegedly told the Soviets about. According to the sources, the second program involves a supercomputer so well known that its capability has been accurately detailed

Continued

in a best-selling novel; and an intelligence-collection satellite. But that satellite was replaced last year by a newer model.

This and other issues raised by disclosures at Pelton's trial have presented a glimmer of how the US advantage in sophisticated technology has allowed it to outpace the Soviets in a crucial area of intelligence gathering. And it has provided rare snapshots of the workings of the National Security Agency, where Pelton worked as an analyst until 1979. The NSA is an agency so secret that even the amount of its annual budget, estimated at $4 billion, is classified.

This super-secret agency operated an underwater intercept program that, by some accounts, had apparently served to enhance a long-standing US superiority in what has been the most enduringly stable leg of the US nuclear triad: US Navy nuclear-powered attack and ballistic-missile submarines, which hold great technological advantages over their Soviet counterparts.

In the other two legs of the triad – nuclear-armed bombers and land-based nuclear missiles – the two superpowers have the ability, theoretically, to neutralize each other with a surprise first strike. With the third leg, however, the US capability serves as a more significant deterrent to a Soviet nuclear attack: the Soviets know that US ballistic-missile submarines can roam the oceans almost at will, all but impervious to Soviet detection and able to deliver a lethal counterblow in the event of a Soviet nuclear attack against the United States.

US undersea advantage

Even without the intelligence compromised by Pelton, the United States holds a substantial undersea advantage, with its use of sophisticated methods for identifying and tracking Soviet submarines, methods that could be employed in case of war to neutralize much of the Soviet submarine fleet.

Some of those methods, the sources said, are related to the second program, Project B, the term used by the prosecution to describe one of the programs Pelton is accused of compromising. It has been referred to at trial only as "valuable information about how quickly the US is able to process and evaluate information" and "the upgrading of the actual equipment that collects Soviet signals."

According to the sources, those are a reference to the satellite that has been replaced and to the Cray supercomputer that millions of readers have learned about from Tom Clancy's 1984 novel, "The Hunt For Red October." Even before publication of the book, thousands of scholars were aware of the computer through the large number of unclassified publications Clancy used in his research.

The Cray, according to these widely available publications, is used by the Navy as well as by NSA to integrate and process data from 'disparate systems that include intercepted communications and the "SOSUS" underwater sensor system that is designed to detect and track Soviet submarines.

Adm. Carlisle A.H. Trost, who was nominated by President Reagan last week to be Chief of Naval Operations, cited that integration effort during public testimony before a Senate committee in 1982. Trost described a new program called the Rapidly Deployable Surveillance System, which would be part of the Integrated Undersea Surveillance System (IUSS). IUSS, in turn, includes the SOSUS system and Surveillance Towed Array System (SURTASS).

Pelton, testifying in his own defense this week, added some details about Project B to the public record. But he said it was of little or no value to the Soviets, insisting that it involved only the replacement of old NSA radio signal demodulators and an enhancement of the "data link" used to transmit signals back to NSA for analysis.

Information for $4.50

Some of the technology that is being shielded from public view is available to anyone who is willing to pay $4.50 for Clancy's widely circulated novel, which has already sold 2.5 million copies.

In the novel, which has been read by President Reagan and other US officials who pronounced themselves astonished at its accurate detail, Clancy brings dry and uninteresting technology to colorful, suspense-filled life in the fictionalized thriller about a defecting Soviet nuclear-missile submarine.

Thanks to that technology, much of which the government considers highly classified, the US Navy is able to locate the wayward Soviet submarine and bring it, along with its classified Soviet secrets, to port, while the Soviet Navy is frustrated in efforts to find its own submarine.

Among other elements of the undersea surveillance system, Clancy cites the existence of the Cray, so powerful that it can process and analyze millions of bits of data from oceans that have been seeded with sophisticated sensing devices to detect Soviet submarine movements.

Describing the fictional top-secret control center, Clancy wrote, "In the basement were a pair of Cray-2 supercomputers tended by twelve acolytes, and behind the building was a trio of satellite ground stations, all up- and downlinks. The men at the consoles and computers were linked electronically by satellite and landline to the SOSUS (sonar surveillance system) system.

"Throughout the oceans of the world, and especially astride the passages that Soviet submarines had to cross to reach the open sea, the United States and other NATO countries had deployed gangs of highly sensitive sonar receptors. The hundreds of SOSUS sensors received and forwarded an unimaginably vast amount of information, and to help the system operators classify and analyze it, a whole new family of computers had to be designed, the [Cray] supercomputers."

By government definition, however, any references to SIGINT (signal intelligence, which includes any electronic and communications intelligence) are considered highly classified – even if they are in the public domain. That argument has been reemphasized by intelligence officials, who have warned reporters that republication of the material could violate a 1950 statute barring disclosure of any SIGINT material.

That same argument appears to be the basis for the government's view of the sensitivity of the trial's so-called Project A, although much less of the detail surrounding that program has surfaced publicly. Project A has been described obliquely in the court

room as "a specific set of equipment" used to intercept signals from "a particular Soviet communications link."

Prosecution threatened

Before the trial, court documents indicated that Project A, compromised by Pelton, was code-named "Ivy Bells." According to a May 26 NBC News report that prompted CIA Director William J. Casey to demand the prosecution of an NBC correspondent, the project was a "top-secret underwater eavesdropping operation by American submarines, inside Russian harbors."

As the trial commenced last month, the Washington Post, after agreeing to a request from President Reagan that it withhold some details of its reporting, further identified the project as a "costly, long-running and highly successful US operation that used sophisticated technology to intercept Soviet communications." The Post, like NBC, said it involved submarines, and that the information Pelton sold the Soviets compromised the project and prompted the Soviets to retrieve the high technology device.

The descriptions by NBC and the Post are similar in some respects to those of a forerunner program, code-named "Holystone," that was detailed in 1975 by the New York Times. Under the headline, "Submarines of US Stage Spy Missions Inside Soviet Waters," the Times described the program as involving the use of Navy submarines inside the Soviet Union's three-mile limit to collect vital data on the capabilities and missile-firing abilities of Soviet submarines.

According to the Times, the US subs "were able to plug into Soviet land communication cables strewn across the ocean bottom and thus were able to intercept high-level military messages and other communications considered too important to be sent by radio or other less secure means." The Times said that the Soviet Union was aware of the program and that two of the US subs had even collided with Soviet subs inside Soviet territorial waters.

References to other underwater intelligence programs have appeared in public or declassified literature. One is "Dark Eyes," an electro-optical viewing system that fits into a submarine's periscope and takes night photographs. At least two others, "Prairie Schooner" and "Sea Nymph," involve interception of Soviet signals.

A boost from technology

Thanks to technological breakthroughs, however, such communications can now be intercepted and relayed back to the United States without US submarines having to remain in the area. The marriage of existing technology to advances in electronics and the growing sophistication of US satellites orbiting far above the Earth led to development of the project Pelton compromised.

Pelton, according to testimony, said the Soviets were already aware of the program's existence. The Post, quoting sources, reported this week that Soviet awareness of the program was based on another collision between a US submarine and a Soviet sub in the Sea of Okhotsk. Pelton, according to Globe sources, told the Soviets how the messages were intercepted and relayed to the high technology device, which in turn relayed the information to a satellite, which transmitted it to NSA.

Also according to Globe sources, and as the Post has already reported, the Soviet debriefing of Pelton led them to retrieve the device and compromise the program.

Like Holystone, its predecessor program, the project compromised by Pelton required US submarines to enter Soviet waters. In the later program, the subs did not have to stay.

According to declassified portions of the Navy's "Special Warfare Master Plan," the Navy has reconfigured some nuclear-powered submarines for such special operations. These subs, called APSSNs, are outfitted with one- or two-man minisubs known as Swimmer Delivery Vehicles.

During his testimony, Pelton acknowledged that he had admitted to FBI agents last year that his disclosures might have placed in jeopardy "a few men who needed to go to and from" the project.

CIA Director Casey has said that Pelton's disclosures destroyed a major source of national security information.

Tapping directly into Soviet communications systems is not a new technique. According to "Wilderness of Mirrors," by David C. Martin, a US program from 1951 to 1956, code-named "Operation Silver," intercepted encoded Soviet messages to and from a command post in East Berlin by tapping into a cable. The operation began after a US intelligence analyst found that coded signals sent through a US cable included faint echoes of the message as it appeared before being scrambled into code.

It is the much more sophisticated technology of the 1980s that has enabled NSA, with its 50,000 employees, to become the world's preeminent intelligence organization. Although most Americans have never heard of NSA, it has long since eclipsed the CIA, and the fabled-in-fiction use of undercover agents, as the source of the country's most useful and timely intelligence.

(Stephen A. Kurkjian of The Globe staff contributed to this report.)