TEMPEST: A Signal Problem

The story of the discovery of various compromising radiations from communications and Comsec equipment.

In 1962, an officer assigned to a very small intelligence detachment in Japan was performing the routine duty of inspecting the area around his little cryptocenter. As required, he was examining a zone 200 ft. in radius to see if there was any "clandestine technical surveillance." Across the street, perhaps a hundred feet away, was a hospital controlled by the Japanese government. He sauntered past a kind of carport jutting out from one side of the building and, up under the eaves, noticed a peculiar thing—a carefully concealed dipole antenna, horizontally polarized, with wires leading through the solid cinderblock wall to which the carport abutted. He moseyed back to his headquarters, then quickly notified the counter-intelligence people and fired off a report of this "find" to Army Security Agency, who, in turn, notified NSA. He was directed to examine this antenna in detail and perhaps recover it, but although the counter-intelligence folks had attempted to keep the carport under surveillance that night, the antenna had mysteriously disappeared when they checked the next day. Up on the roof of the hospital was a forest of Yagi's, TV antennae, all pointing towards Tokyo in the normal fashion, except *one*. That one was aimed right at the U.S. cryptocenter.

You may recall the highly publicized flap which occurred in 1964 when more than 40 microphones were discovered in the U.S. embassy in Moscow. Most people were concerned about all the conversations that may have been overheard and the resultant compromise of our diplomatic plans and intelligence activities associated with the embassy. We were concerned with something else: What could those microphones do to the cryptomachines used there? And what were the unpublicized gadgets also found with microphones for? Why was there a large metal grid carefully buried in the cement of the ceiling over the Department of State communications area? A grid with a wire leading off somewhere. And what was the purpose of the wire that terminated in a very fine mesh of smaller hair-like wires? And, while we were at it, how did these finds relate to other mysterious finds and reports from behind the Curtain—reports dating clear back to 1953?

Why, way back in 1954, when the Soviets published a rather comprehensive set of standards for the suppression of radio frequency interference, were those standards much more stringent for their teletypewriters and other communications equipment than for such things as diathermy machines, industrial motors, and the like, even though the teletypewriters were much quieter in the first place?

Behind these events and questions lies a long history beginning with the discovery of a possible threat, the slow recognition of a large number of variations of that threat, and, lumbering along a few months or a few years afterwards, a set of countermeasures to reduce or eliminate each new weakness that has been revealed.

The Problem Defined

To state the general nature of the problems in brief: Any time a machine is used to process classified information electrically, the various switches, contacts, relays, and other components in that machine may emit radio frequency or acoustic energy. These emissions, like tiny radio broadcasts, may radiate through free space for considerable distances—a half mile or more in some cases.

Or they may be induced on nearby conductors like signal lines, power lines, telephone lines, or water pipes and be conducted along those paths for some distance— and here we may be talking of a mile or more.

When these emissions can be intercepted and recorded, it is frequently possible to analyze them and recover the intelligence that was being processed by the source equipment. The phenomenon affects not only cipher machines but *any* information-processing equipment—teletypewriters, duplicating equipment, intercomms, facsimile, computers—you name it. But it has special significance for cryptomachines because it may reveal not only the plain texts of individual messages being processed but also that carefully guarded information about the internal machine processes. Thus, conceivably, the machine could be radiating information which could lead to the reconstruction of our daily changing keying variables—and from a Comsec viewpoint, that is absolutely the worst thing that can happen to us. This problem of compromising radiation we have given the covername TEMPEST.

Discovery by Bell Lab

Now, let's go back to the beginning. During World War II, the backbone systems for Army and Navy secure teletypewriter communications were one-time tapes and the primitive crypto-equipment SIGTOT. For encrypting, the Services used a Bell-telephone mixing device, called a 131-B2. When one of these mixers was being tested in a Bell laboratory, a researcher noticed, quite by accident, that each time the machine stepped, a spike appeared on an oscilloscope in a distant part of the lab. After he examined these spikes more carefully, he found that he could read the plain text of the message being enciphered by the machine!

Bell Telephone faced a dilemma. They had sold the equipment to the military with the assurance that it was secure, but it wasn't. The only thing they could do was to tell the Signal Corps about it, which they did. There they met the charter members of a club of skeptics who could not believe that these tiny pips could really be exploited under practical field conditions. They are alleged to have said something like: "Don't you realize there's a war on? We can't bring our cryptographic operations to a screeching halt based on a dubious and esoteric laboratory phenomenon. If this is really dangerous, prove it." So, the Bell engineers were placed in a building on Varick Street in New York. Across the street and about 80 feet away was Signal Corps' Varick Street cryptocenter. The engineers recorded signals for about an hour. Three or four hours later, they produced about 75% of the plain text that was being processed—a fast performance, by the way, that has rarely been equalled.

The Signal Corps was impressed by this display and directed Bell Labs to explore this phenomenon in depth and provide modifications to the 131-B2 mixer to suppress the danger. In a matter of six months or so, Bell Labs had identified three separate phenomena and suggested three basic suppression measures:

(a) Shielding (for *radiation through space, and magnetic fields*)
(b) Filtering (for *conducted signals on power lines, signal lines, etc.*)
(c) Masking (for either *space-radiated or conducted signals,* but mostly for space)

Bell Labs went ahead and modified a mixer, calling it the 131-A-1. In it they used both shielding and filtering techniques. Signal Corps took one look at it and turned thumbs down. The trouble was, to contain the offending signals, Bell had to virtually encapsulate the machine. Instead of a modification kit that could be sent to the field, the machines would have to be sent back and rehabilitated. The encapsulation caused problems of heat dissipation, made maintenance extremely difficult, and hampered operations by limiting access to the various controls.

Instead of buying this monster, the Signal Corps resorted to the only other solution they could think of. They went out and warned commanders of the problem, advised them to control a zone about 100 feet in diameter around their communications center to prevent covert interception, and let it go at that. And the cryptologic community as a whole let it go at that for the next seven years or so. The war ended; most of the people involved went back to civilian life; the files were retired, dispersed, and destroyed. The whole problem was, apparently, forgotten. Then, in 1951, the problem was, for all practical purposes, rediscovered by CIA when they were toying with the same old 131-B2 mixer. They reported having read plain text about a quarter mile down the signal line and asked if we were interested. Of course, we were. Some power line and signal line filters were built and immediately installed on these equipments and they did the job pretty well as far as conducted signals were concerned. Space radiation continued unabated, however, and the first of many "radiation" policies was issued in the form of a letter from AFSA to all Sigint activities, requiring them to:

1. Control a zone 200 feet in all directions around their cryptocenters, or
2. Operate at least 10 TTY devices simultaneously (the idea of masking; putting out such a profusion of signals that interception and analysis would be difficult), or
3. Get a waiver based on operational necessity.

The Sigint community conformed as best it could; and, in some instances, general-service communicators adopted similar rules. The figure of 200 feet, by the way, was quite arbitrary. It had not been determined because we had hard evidence that, beyond that distance, interception was impractical; rather, it was the largest security zone we believed the majority of stations could reasonably maintain, and we knew that, with instrumentation then available, exploitation at that range would, at best, be exceedingly difficult.

At the same time that we were trying to cope with the 131-B2 mixer, we began to examine every other cipher machine. *Everything* tested radiated, and radiated rather prolifically. With rotor machines, the voltage on their power lines tended to fluctuate as a function of the number of rotors moving, and so a fourth phenomenon, called *power line modualtion,* was discovered.

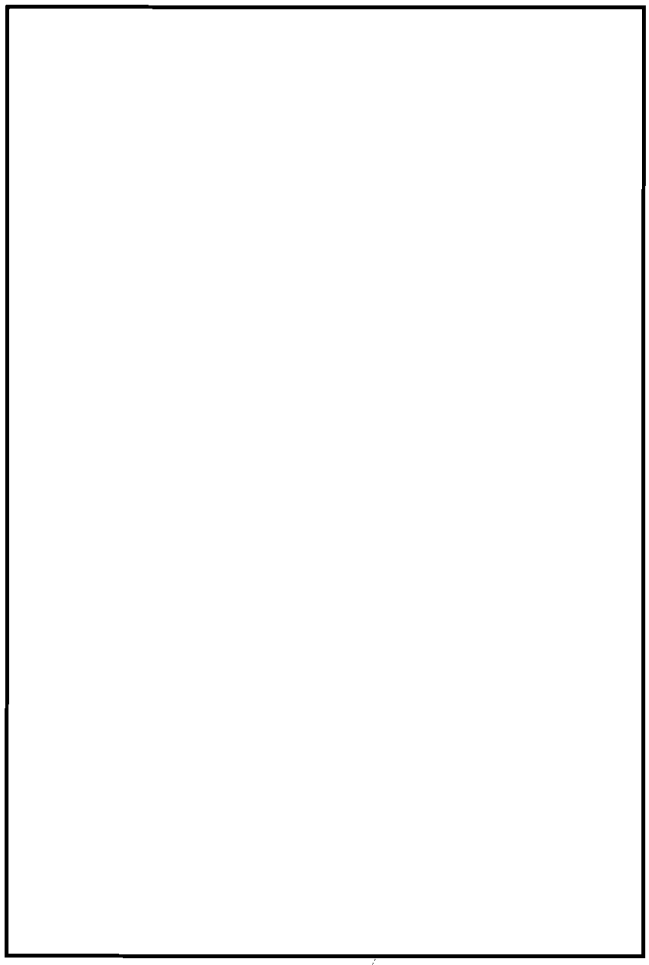
Progress in examining the machines and developing suppression measures was very slow. By 1955, however, a number of possible techniques for suppressing the phenomena had been tried. Filtering techniques were refined somewhat; teletypewriter devices were modified so that all relays operated at once and only a single spike was produced with each character, instead of five smaller spikes, representing each baud, but the size of the spike changed with each character produced, and the analysts could still read it quickly. A "balanced" ten-wire system was tried which would cause each radiated signal to appear identical, but to achieve and maintain such balance proved impractical. Hydraulic techniques—to replace the electrical—were tried and abandoned, and experiments were made with different types of batteries and motor generators, in attempts to lick the power-line problem. None was very successful.

During this period, the business of discovering new TEMPEST threats, or refining techniques and instrumentation for detecting, recording, and analyzing these signals, progressed more swiftly than the art of suppressing them. Perhaps the attack is more exciting than the defense—something more glamorous about finding a way to read one of these signals than going through the drudgery necessary to suppress that whacking great spike first seen in 1943. At any rate, when they turned over the next rock, they found the acoustic problem under it. Phenomenon No. 5.

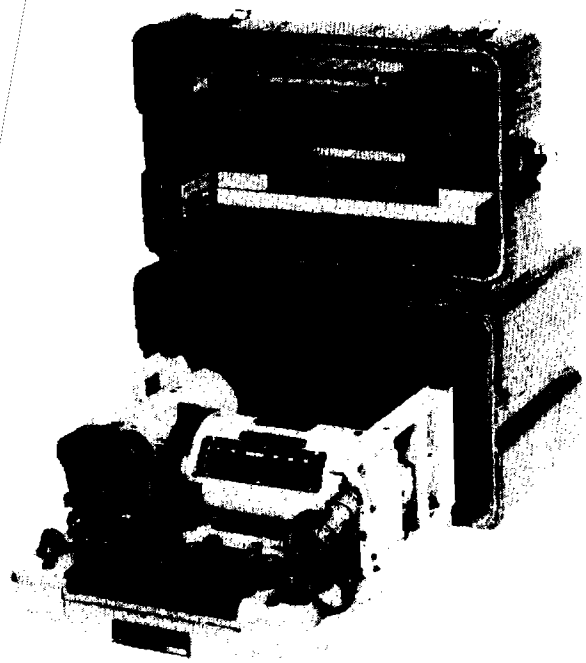
Acoustics

We found that most acoustic emanations are difficult to exploit if the microphonic device is outside of the room containing the source equipment; even a piece of paper inserted between, say, an offending keyboard and a pick-up device, is usually enough to prevent sufficiently accurate recordings to permit exploitation. Shotgun microphones—the kind used to pick up a quarterback's signals in a huddle—and large parabolic antennae are effective at hundreds of feet—if there is a direct shot at the equipment. The acoustic threat is, therefore, confined to those installations where the covert interceptor can get some kind of microphone—such as an ordinary telephone that has been bugged or left off the hook—in the same room with the information-processing device. We also discovered that, when the room is "sound-proofed" with ordinary acoustic title, the job of exploitation is easier because the sound-proofing cuts down reflected and reverberating sound, providing clearer signals. A disturbing discovery was that ordinary microphones, probably planted to pick up conversations in a cryptocenter, could detect machine sounds with enough fidelity to permit exploitation. And such microphones were discovered in Prague, Budapest, Warsaw and, of course, Moscow.

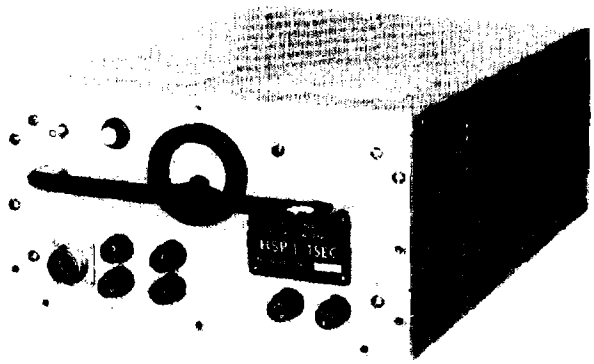
Seismics



Flooding



The TSEC/KL-7, Electromechanical Literal Cipher Machine, a crypto-equipment long in use by the U.S. and its Allies



The TSEC/KL-7A, the version of the KL-7 modified

Anomalies