A Major Comsec Challenge: Secure Voice

Washington DC's first private telephone line—between the office of the Army's chief signal officer and Fort Myer, Virginia (then Fort Whipple)—was connected in October 1877, just 18 months after Alexander Graham Bell received the patent on his invention. Yet, strange as it may seem, Herbert Hoover was the first U.S. President to have a telephone installed at his White House desk. His predecessors Wilson, Harding and Coolidge used a phone booth down the hall. Over fifty years elapsed between the first military application of the telephone and the installation of a handset on the President's desk. Couldn't happen today, you say? Well, almost.

The first cryptographically secure voice circuit became operational toward the latter part of World War II. Yet it was not until some 20 years later that the President was able to place a secure telephone call without leaving his office. Why the delay?

Secure Voice Lag

With voice communications in the form of both radio and telephone being commonplace items in American homes for more than four decades, why has secure voice lagged so far behind? And lag behind it has! As of this date, less than 1% of the telephones in the Department of Defense are cryptographically secured. And only an estimated 5-8% of the tactical military radios in the U.S. Army are currently secured—a fact which allowed the out-gunned, uneducated, relatively ill-equipped army of the Viet Cong to repeatedly degrade the effectiveness of one of the most powerful fighting forces in the world through the imaginative use of communications intelligence derived from our plaintext traffic. Why, then, have we not secured more of our voice communications?

Secure Telephone Communications

Trying to pipe encrypted voice over a pair of telephone wires is like trying to put all of the Los Angeles freeway traffic on a rural Kansas road at the same time. Whereas normal telephone conversations require only the rural road (a pair of wires) for transmission, secure voice requires anywhere from five to twenty times more electronic space or, in telephone language, "bandwidth."

The reason is simple enough: the process of converting the voice signal to a form suitable for encryption increases significantly the size (bandwidth) of the original signal. So far the available choices for getting around this problem have been limited to two.

One of these is to force the secure voice signal down the rural road by cutting away all but the absolutely essential elements of original voice signal before it is encrypted. Then the expansion caused by preparing the signal for encryption only returns it to its original size. This is referred to in the communications world as the "narrowband" approach. Circuits of this type are being used today, but the results are poor. The voice takes on a choppy, Donald Duck sound. If you have ever talked long distance over the AUTOSEVOCOM telephones, the chances are that your call was encrypted with this technique and you probably had some difficulty in understanding and being understood.

A second choice uses the wider signal as is. This solves the voice quality problem but has its own drawback—it costs far too much for most applications. The high cost stems primarily from the fact that this solution, conceptually, includes leasing or buying commercial telephone lines and "stacking" them so that together they can accommodate the wider signal. This "wideband" approach is also being used today, but the cost is such that it has to be limited to situations where good voice quality

Cryptologia Spectrum Fall 1974

is essential and the very high line rental expense can be justified.

A different crypto-equipment is required for each of these two voice encryption methods. The AUTOSEVOCOM system used today to provide secure voice for DoD and some other U.S. Government Departments and Agencies, uses a mixture of both techniques. This system accounts for the 1% secure telephones in DoD, a figure mentioned earlier. The unfortunate fact is that it simply costs too much to do more.

But it is painfully obvious that not securing these communications is costly, too. And the biggest part of the cost is not measurable in dollars. The intelligence value of the information readily available from our unsecured voice communications is tremendous—so much so that the problem has received attention at the top levels of government. In 1971 the United States Communications Security Board became sufficiently concerned to establish a national policy stating that "all military voice radio systems and civil governmental communications which carry traffic of significant intelligence value will be secured." This has had the effect of increasing the priority of efforts in NSA and throughout the rest of the government to overcome the obstacles which so far have made widespread secure voice economically infeasible. The new policy was a major step in the right direction, but there was still a lot of ground to cover, much of it technical.

The ideal solution, of course, would be to find an economical way to encrypt speech without having to increase the size of the signal. Among other benefits, this would allow full use of the massive telephone communications system already existing in this country and abroad. In effect, any telephone handset anywhere could then be converted for use as a secure voice terminal. Accelerated research in both government and private industry is underway now, but there are still some formidable technical and cost problems to be solved. We cannot expect to see production quantities of operational hardware before the early 1980s.

But must we wait until then to begin to do something? The answer, fortunately, is no. There are some things that can be done now to deny to the unauthorized listener a large volume of unsecured voice communications transmitted over microwave links, which are now both easily accessible to him and very lucrative in terms of intelligence content.

To understand this situation it is only necessary to know that it is common practice both in the commercial and government-owned systems for conversations from many individual telephone instruments to be bundled together at one point and transmitted en masse by microwave to another point, where the conversations are then sorted and distributed by wireline. This is done in both the U.S. and abroad. It is simple enough for an interceptor to sit somewhere near the microwave transmission path and record the entire bundle with relatively unsophisticated, inexpensive equipment. He can even select the channels of special interest to him for special attention. He spends little and collects much.

It might be of interest to point out that the telephone calls of the government organizations in Washington, including those of the Pentagon, State Department, the White House, CIA and others, are transmitted by microwave to points outside the Washington area. It is probably not just coincidence that the Soviets acquired real estate on or near the transmission most of these microwave links and have tried to acquire more.

NSA25X1
NSA25X3

[redacted]

At the moment, the application of this bulk encryption technique is limited. We do it by combining an existing crypto-equipment with some commercially manufactured components already available. With this system we can now bulk encrypt 24 voice conversations simultaneously. Today, to encrypt more channels we have to add more equipments, which is costly. Thus, as in other voice encryption techniques, economics necessarily plays an important role in limiting its application.

Some rather sophisticated studies have been conducted in an attempt to rank the existing U.S. microwave links around the world in terms of the degree of threat against them, the extent of their vulnerability to that threat, and the intelligence value of their products. In this way a strategy for gaining maximum benefit from limited resources has been applied. And a crypto-equipment capable of operating at up to ten or more times the speed

of the current system is in the final developmental stages. When this system (WALBURN) is implemented, it will permit the encryption of more channels at less cost per channel.

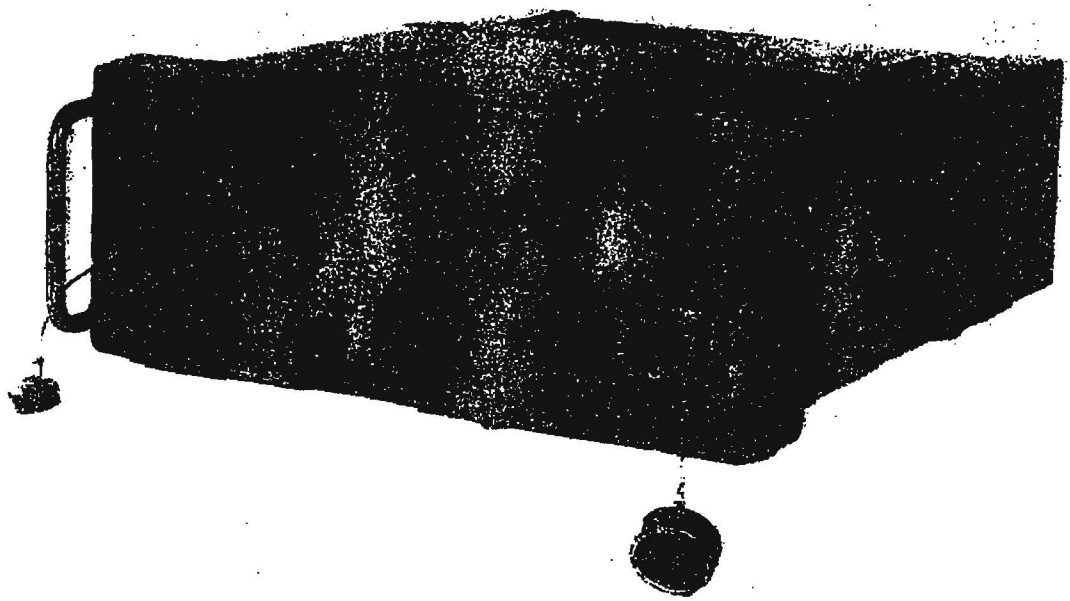
In summary, then, comparatively few of our telephone communications are now secured. These unsecured communications are known to be a major source of intelligence for foreign interceptors and an easy target for spoofing or imitative deception. The problem in providing security for these communications is both technical and economic, and a permanent solution is not expected before the early or mid 1980s. In the interim, bulk encryption of selected microwave links will deny the interceptor some of the more lucrative and accessible sources now available to him at relatively little cost or risk.

Secure Radio

But not all voice communications have to be done by telephone; there is also the radio. The predominant applications here are in tactical military operations where the transmissions are limited to a relatively local area. Although there are no transmission lines to limit the space available for a radio signal, all is not peaches and cream, for, in the HF portion of the radio frequency spectrum, for instance, where commercial AM radio operates and long-range transmissions are possible, the spectrum is very crowded. Here the extra bandwidth required by the encryption process is a very real limitation. To get around this we have developed a crypto-equipment called PARKHILL, which secures the voice signal without expanding the signal size. The voice quality is very good and the costs, while not insignificant, are still relatively attractive. The Secretary of Defense approved a procurement program that will achieve security for 100% of the critical radio nets operating in the HF portion of the radio frequency spectrum. Production deliveries are scheduled to begin in the latter part of 1976. PARKHILL does, however, pose some problems: it will be a nondigital equipment in what will eventually become a digital communications world. Research on alternatives for securing HF radios is, of course, continuing.

In the UHF & VHF portions of the radio frequency spectrum the scene changes. Here there is enough bandwidth available to accommodate the extra amount required by the encryption process. As a result, encryption can be added to VHF and UHF radios easily without either prohibitive line rental costs or sacrifices in voice quality. At present, this is being done simply by connecting one piece of encryption equipment to the transmitting radio and another to the receiving radio. Though the only extra costs are those of the encryption equipment themselves, this still represents a relatively large investment per net and, along with power, size and weight, is a major reason why no more than about 8% of the current inventory of military tactical radios is secured.

During World War II no tactical voice radios were secured. The technology of the day simply did not permit



PARKHILL (KY-65/75), which is designed to secure HF radios, will be operational in 1976.

it. It took ten trucks (literally) to carry one terminal of our only secure voice equipment from the beachhead to General Eisenhower's headquarters in Paris. Secure voice for tactical use was completely unthinkable; a manpack unit was unimaginable.

The transistor technology of the fifties and integrated circuits of the sixties changed the picture, and at the time of the conflict in Southeast Asia, NSA rushed into production to provide tactical secure voice equipments to operate with the current inventory of military radios. This equipment, NESTOR, was produced in three forms, for use in an airplane, on board a ship, or on a ground vehicle or a man's back. All three were cryptographically compatible—that is, they could talk to each other. It is these equipments that account for the 8% of the U.S. military tactical radios that are secured today. Although NESTOR has some recognized shortcomings (excessive weight, excessive power requirements, susceptibility to fading and interference and a cryptoprinciple developed in the 1950s), production of this equipment has continued into 1974.

No new tactical voice crypto-equipments have been introduced into the inventory since NESTOR. R&D efforts since the initial fielding of NESTOR, however, have been continuous. The evolution of large-scale integration—Metallic Oxide Semi-Conductor (MOS) technology—during the past decade opened the door to the development of cryptographic hardware offering many important advantages over the NESTOR family of equipments.

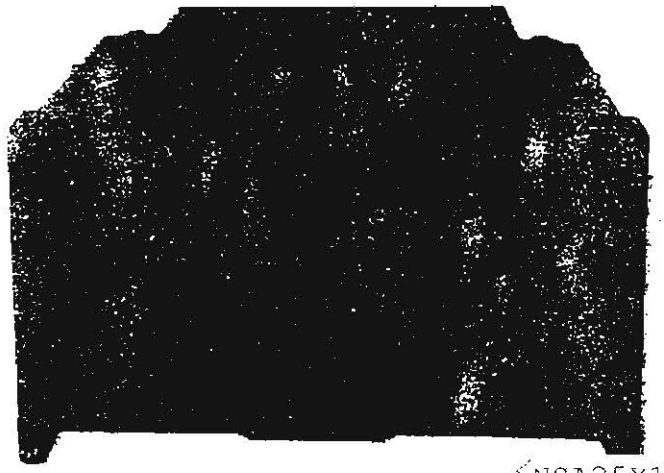
An improved system, VINSON, has completed the research-and-development phase in NSA and will be tested by the military services during 1975. It is expected to be fielded in production quantities for operational use in 1977.

The introduction of the VINSON equipment is significant in the evolution of voice security. Not only does it represent the end of more than ten years of new equipment drought, but in a way it heralds the beginning of a new era in tactical voice security. In addition to impressive reductions in size, power consumption and weight, VINSON offers a number of important improvements over NESTOR—improved security through the use of a new cryptoprinciple; [redacted] better voice quality; [redacted] and greater immunity to fading and interference.

The Future

The cryptoprinciple of VINSON and the technology it fostered have been incorporated into experimental Comsec modules which can be plugged into radios to make them secure and on devices in which the encryption circuitry is interwoven into the radio circuitry itself. These will effect even greater savings in cost, weight and size. And most importantly, we can be sure of increased utility by the communicators. These equipments will be available for use in the late 1970s and early 1980s.

The procurement program for tactical secure voice systems over the next five years is large—enough so, in fact, that it is expected to provide security for 100% of the critical tactical non-wireline communication nets when implementation is completed.



NSA25X1
NSA25X3

VINSON: Wideband tactical secure voice equipment expected to become operational in 1977.

*****

The status of this country's voice security is undeniably poor at the moment. Secure voice is the single most important area in which improvement is needed if the U.S. is to achieve a satisfactory Comsec posture. Fortunately, the future looks much brighter. The turn of the decade should also be a turning point for U.S. voice security. By then we will have the equipment to secure the telephones handling the information of the highest intelligence value to foreign interceptors; we will have bulk encrypted the more sensitive microwave links; we will have perfected a system for assuring long-term security protection for HF radio communications; and we will have the newer, smaller and improved techniques for securing the multitude of VHF/UHF tactical radios throughout the military services. Then, by about the mid-80s the Services will begin to field a system called TRI TAC, which will provide, through a system of centrally located switches, a completely secured system

cryptologically compatable with existing equipments, which will permit subscriber-to-subscriber security for all calls, both local and long distance, analog and digital, voice and data.

In one sense, the cost for securing our voice communications will be high. The U.S. Government price tag for secure voice equipment over the next five years exceeds a half-billion dollars—as much as the government has spent on all types of Comsec equipment combined in the last ten years. In return, we will realize a quantum jump in our ability to secure voice communications on a massive scale.

[redacted]

Until the bulk of Federal electrical communications is encrypted automatically without user option, our far-flung

[redacted]

NSA25X1
NSA25X3
P.L. 86-36

[redacted] who holds a degree in Industrial Engineering from the University of Illinois, is currently serving as Chief of the Briefing Management Staff of the Management Staff of the Communications Security Organization. He has served as Assistant Inspector General and held various managerial and staff positions in Comsec. He is a certified professional in the engineering, Comsec, resources management and the industrial production career fields.