



Learning from the Enemy The GUNMAN Project



This publication presents a historical perspective for informational and educational purposes, is the result of independent research, and does not necessarily reflect a position of NSA/CSS or any other U.S. government entity.

This publication is distributed *free* by the National Security Agency. If you would like additional copies, please email history@nsa.gov or write to:

Center for Cryptologic History
National Security Agency
9800 Savage Road, Suite 6886
Fort George G. Meade, MD 20755

Sharon A. Maneki, senior historian at the Center for Cryptologic History, retired in 2012. She has an M.A. in history from Jersey City State College.

Cover: U.S. Embassy in Moscow

Learning from the Enemy

The GUNMAN Project

Sharon A. Maneki



Center for Cryptologic History

First edition published 2012; Second edition 2018



U.S. embassy in Moscow at the time of Project GUNMAN

Introduction

On 25 March 1985, *CBS Nightly News* broke the following shocking story:

News anchor Dan Rather: “In another U.S.-Soviet development, Pentagon correspondent David Martin has been told how Soviet secret police in Moscow have been getting the latest word on sensitive U.S. embassy documents even before U.S. officials read them.”

David Martin: “Informed sources tell CBS News that for at least one year, and probably longer, the American embassy in Moscow was the victim of a sophisticated electronic spy operation which gave Soviet leaders an inside look at what U.S. diplomats were doing and planning. Soviet agents secretly installed tiny sensing devices in about a dozen embassy typewriters. The devices picked up the contents of documents typed by embassy secretaries and transmitted them by antennas hidden in the embassy walls. The anten-

nas, in turn, relayed the signals to a listening post outside the embassy.

“Depending on the location of the bugged typewriters, the Soviets were able to receive copies of everything from routine administrative memos to highly classified documents.

“One intelligence officer said the potential compromise of sensitive information should be viewed with ‘considerable seriousness.’

“Another intelligence expert said no one knows for sure how many or what secrets were compromised. A third official called the entire affair a fiasco.”¹

How accurate was the CBS report? This brochure examines the nature of the Soviet electronic penetration and the damage assessment of Soviet access to typewriters at the U.S. embassy in Moscow. This history of Project GUNMAN will also answer such questions as how the typewriter bugs were discovered and how they worked.

Countries have spied on each other by gathering information from embassies for centuries. The United States and the Soviet Union were, of course, archenemies during the Cold War (1945 to the fall of the Soviet Union in 1991), and there is a long history of attempts by the Soviets to gain access to information from the U.S. embassy and its diplomatic apparatus. Perhaps the most famous incident of Soviet espionage was the Great Seal implant.

On 4 August 1945, Soviet schoolchildren presented a carving of the Great Seal of the United States to Averell Harriman, the U.S. ambassador to the Soviet Union. The carving hung in Spaso house, the ambassador’s residential office in Moscow, until 1952, when the U.S. State Department discovered that hidden inside the carving was a microphone that the Soviets turned on at will. This bug was not a standard microphone and could not be detected unless it was in use. For six years the Soviets were able to eavesdrop on the conversations of the U.S. ambassador.² The Soviet threat to U.S. embassy security was both well documented and real.

The typewriter bugs marked a new level of sophistication because they were electromechanical. For the first time, the Soviets gathered information from a piece of equipment that held written plaintext information. Prior to the discovery of these bugs, the United States believed that the Russians had used only room audio bugs with microphones or listening devices to eavesdrop on American embassy activities. The Soviet Union valued eavesdropping and thus developed ingenious methods to accomplish it.

The 1980s were a period of strained relations between the United States and the Soviet Union. One manifestation of those strains was Project GUNMAN, which involved the replacement of U.S. embassy equipment in Moscow and the discovery and evaluation of typewriter bugs. Those bugs were not the only threat to the U.S. embassy in Moscow. The United States began to build a new office for its Moscow embassy in 1979. The building, however, was riddled with bugs, and the U.S. government eventually rejected it. That story is a subject for another study. This is the story of Project GUNMAN and NSA's role in it.

Organizations with intelligence responsibilities must be able to respond quickly and creatively to unforeseen threats. How did NSA respond to this Soviet threat? To answer that question, this brochure examines the role of NSA leadership and its ability to move a bureaucracy into action. To curtail future threats, intelligence organizations must also maintain the ability to learn from the activities of their enemies. What techniques did NSA use to learn from Soviet bugging efforts?

The Catalyst

The *CBS Nightly News* 25 March 1985 report that announced to the world that the Soviets had penetrated typewriters in the U.S. embassy in Moscow was correct in that the attack took place. According to CBS, “the bugs might still be in place had it not been for a warning from a friendly government whose own embassy had been the target of a similar eavesdropping operation.”³

After learning about the bug at the foreign embassy in August 1983, the Director of NSA (DIRNSA), Lieutenant General Lincoln Fauser, sent analysts from R9, the Research and Development organization, and from the Communications Security (COMSEC) organization to examine the implant the other nation had discovered. It was unusual for the Research and COMSEC organizations to have a reason to work together. This was the first of many examples of collaboration that developed between the two entities to uncover and understand the GUNMAN threat.

The analysts found that the foreign embassy implant (which proved to be very different from the ones later found in the U.S. embassy) represented a major Soviet technological improvement over previous efforts. The development of this bug required competent personnel, time, and money. The very manufacture of the components required a massive and modern infrastructure serviced by many people. This combination of resources led to the assumption that other units were available.⁴

The other nation’s bug, which was not in typewriters but in other types of equipment, could be rapidly and easily installed by nontech-



An IBM Selectric typewriter like those used in the U.S. embassy in Moscow in the 1980s. The Soviets placed electronic bugs inside many of the machines.

nical personnel; it resisted detection by conventional methods; and it was wireless and remotely controlled. Search by disassembly and visual inspection, when conducted by any but the best-trained technicians, normally would be unproductive. All concluded that if the Soviet KGB would go to these lengths against a Western ally, then certainly the United States could expect to be a high-priority target.⁵ The warning was the catalyst for NSA action.

Under the leadership of Walter Deeley, the deputy director for communication security, and the chief of R9, a division in the Research and Development organization, NSA management developed a plan to remove, replace, and examine telecommunications and information processing equipment at the U.S. embassy in Moscow.

NSA was to handle all aspects of the plan on an absolutely need-to-know basis. NSA wanted to remove all of the equipment so that it could be examined stateside more thoroughly than was possible on embassy grounds. NSA also wanted to keep the Soviet Union from learning about the effort and interfering with U.S. objectives. The

Soviets had a history of poisoning or using other means to injure technicians from other countries who investigated bugs in their respective embassies.⁶

General Faurer did not want to bring this plan to the State Department because relations between NSA and State were poor. NSA had been writing critical reports about inadequate security in State Department facilities for several years. Faurer also believed that the Central Intelligence Agency (CIA) would mishandle the NSA plan.⁷

NSA briefed the secretary of defense, Caspar Weinberger, on the threat of a possible bug in U.S. embassy equipment and its proposed plan of action. Weinberger said that this problem should be brought to the attention of the president immediately. The individual whom Deeley assigned to work with the White House later explained that the approval from President Ronald Reagan for the NSA plan of action came in record time. The NSA representative briefed Ken DeGraffenreid (the senior director of intelligence programs on the National Security Council). Next, he briefed Admiral John Poindexter (the deputy national security adviser, who became the national security adviser in 1985). Admiral Poindexter wrote the necessary memorandum, and President Reagan signed the document of authorization for the GUNMAN project in February 1984.

Even after presidential approval, knowledge of GUNMAN was still tightly held within the government. NSA's White House liaison further explained that Admiral Poindexter told him to brief Secretary of State George Schultz and Director of Central Intelligence William Casey, and no one else. He pleaded to brief Lawrence Eagleburger (undersecretary for political affairs) because he feared that he could not reach the secretary of state if NSA needed help in gaining the cooperation of the State Department. After much begging, Poindexter relented. This incident is an indication of the high level of concern for security within the U.S. government.⁸

Developing in just a few months a detailed plan for removing, replacing, and examining every piece of telecommunications and information processing equipment at the Moscow embassy, and getting presidential approval to proceed, was a significant achievement.

This was a testament to the leadership of Walter Deeley, a manager who took risks and made decisions. Right from the start of GUNMAN, the Research and COMSEC directorates worked together. Overcoming bureaucratic hurdles was also possible because during the 1980s the Reagan administration had an overarching concern with the Soviet threat to the United States.

The Race to Remove and Replace Embassy Equipment

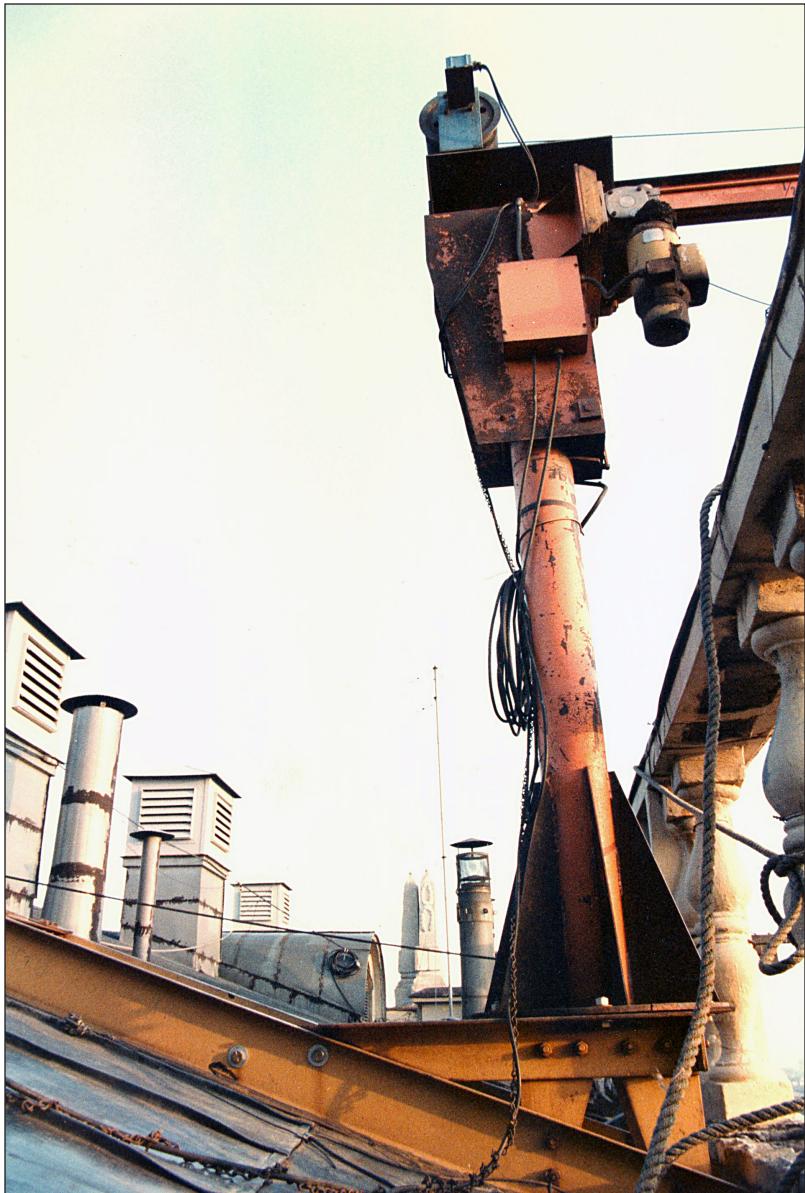
The first goal of the GUNMAN project, to replace all of the electronic equipment in the U.S. embassy in Moscow, was a daunting challenge. Electronic equipment included teletype machines, printers, computers, cryptographic devices, and copiers—in short, almost anything that plugged into a wall socket. NSA staff had to move quickly to replace equipment to avoid tipping off the Soviets. According to an analyst who was involved with the procurement and shipment of the upgraded equipment to Moscow, Walter Deeley gave the staff 100 days to complete this phase of the project.

The analyst explained that the first problem they faced was the lack of a centralized inventory at the embassy. The problem was further complicated because individual departments had software tailored to their specific needs. For instance, NSA technicians could not simply replace all of the Wang computers. Keeping track of the various software was hard enough, but keeping track of all of the variations was a nightmare. With the assistance of a few trusted communication center embassy employees, NSA was able to obtain diagrams and blueprints of equipment. However, analysts frequently found that the original diagram did not match the equipment that had been actually delivered. Security concerns were another challenge identified by the NSA technicians. They could not just show up to take an inventory because they could not risk alerting the Soviets. Instead, telecommunication personnel from NSA were sent to the embassy. They quickly obtained the information that was needed to procure the necessary equipment.⁹



Rear of U.S. embassy in Moscow. Equipment was lifted using a roof hoist, since the Soviets had shut off the elevator.

NSA used a variety of methods to quickly purchase similar or upgraded equipment for the embassy. Approximately 40 percent of the equipment had to be purchased, while 60 percent was available from the Agency and other sources. NSA was unable to obtain 250



Crane winch on roof of U.S. embassy, Moscow,
used to maneuver equipment

IBM Selectric typewriters required by the embassy in part because of their power requirement. The Soviet Union used 220-volt 60-cycle electricity. Typewriters were not available from European sources, and the IBM factory in Lexington, Kentucky, had depleted most of its stock. NSA was able to acquire only 50 typewriters, so they replaced typewriters that were used in the most sensitive areas of the embassy. NSA was able to meet the requirements for all other equipment.¹⁰

Because of the need for fast delivery to the embassy once the equipment arrived in Moscow, NSA had to be certain that each piece of equipment worked. There would be no time to repair anything. NSA also wanted to make sure that the replacement equipment was not tampered with while en route. The COMSEC organization took a number of steps not only to safeguard the equipment in transit, but also to determine whether it was tampered with when it was brought back for periodic examination after being operational in the field. For the next two months, personnel primarily from S65 (COMSEC Standards and Advanced Technology Division) and T2 (Technology Directorate) worked feverishly to prepare the equipment for shipment. This was another example of collaboration between NSA organizations.

A separate area on the NSA Washington campus, known as the T Motor Pool area, contained four trailers that were used to stage the equipment. T2 used the first trailer to test each piece of equipment to ensure its proper function. In the second trailer, COMSEC personnel inspected each item by x-ray. They also disassembled every item to record anomalies that would be stored in their standards library for future reference during examination when the equipment came back from the field. They performed special procedures in the third trailer and used the last one for storage.

Every possible precaution was taken during the entire project to ensure that the replacement equipment remained secure. NSA staff guarded against tampering by using several levels of detection devices. Some methods were applied to the equipment itself, while others involved the packaging of the equipment. Conformal coating was an



Equipment being delivered to trailers at NSA from Moscow. The burlap wrap indicating diplomatic cargo was secured with tamper-proof staples and seals.

example of a method applied directly to the equipment. This procedure involved the application of material to components that would reveal tampering attempts. Equipment was sealed in special plastic bags that could not be replicated in the Soviet Union. Some boxes contained special equipment. To the best of NSA's knowledge, the Soviets did not interfere with any of the equipment that was shipped to the embassy or returned to Fort Meade.¹¹

The staff took extraordinary measures to ensure the security of the equipment during its shipment to the embassy. In preparation for shipment, boxes of equipment were placed in crates, which were wrapped in burlap. Burlap signified that these items were to be treated as U.S. diplomatic cargo and would not be subject to inspection by Soviet customs officials. As a further security measure, the burlap was stapled onto each crate. Even the staples in the burlap and the seals on the straps of the crates had microscopic markings which were unlikely to be correctly duplicated in the event of tampering attempts. Next, the crates were placed in trailers for easier transport and additional security. Special light sensors were installed in each

trailer that recorded the dates the trailer door was opened by sensing a change in light intensity.

The equipment was shipped to Moscow in May 1984. From NSA, the Armed Forces Courier Service shipped the equipment to Dover Air Force Base in Delaware. An example of attention to every detail of security was the rental of a special crane to load the plane. The regular crane was not operational when the equipment arrived. The flight was scheduled to leave in three hours. The equipment could not miss that flight because NSA personnel did not want to store it at Dover. Therefore, the plane was loaded using a rented crane.

Two cleared couriers accompanied the equipment, which was flown by military transport to Frankfurt, Germany. The equipment was stored and guarded by U.S. personnel at a warehouse in Germany until it could be flown into Moscow. This was necessary because there was no place at the U.S. embassy in Moscow to store 10 tons of equipment at one time.

The equipment was flown into Moscow in stages on a Lufthansa aircraft, a common State Department procedure. The Soviets were not surprised by an influx of equipment to the embassy because such activity was typical in the spring. The only way to get equipment into the embassy was by using a hoist from the outside. This hoist was frozen all winter and inoperable, making larger deliveries necessary in the spring. However, the Soviets turned off the electricity to the embassy elevator for preventive maintenance after the first day of the influx of equipment. Most of the approximately 10 tons of equipment that went into the embassy and the 11 tons that came out had to be carried manually. (Note: Some sources maintain that less equipment went into the embassy as replacements because they were upgraded models. Other sources maintain that 11 tons came out of the embassy because there were bags of sensitive trash that NSA wanted to examine back at Fort Meade.)

The true nature of the GUNMAN project was successfully masked from most embassy employees. Ambassador Arthur Hartman learned about the project via a handwritten note that NSA rep-

representatives personally delivered when they arrived at the embassy. Ambassador Hartman announced that there was to be an upgrade of embassy communications, which accounted for all of the replaced equipment.¹² Embassy personnel were happy because they received new equipment and upgrades without having to use any of their own funding.¹³

The embassy environment made the swap of equipment even more difficult. A State Department employee who was the deputy chief of the communication center at the Moscow embassy described the facility as old, decrepit, and outdated. As an employee in the U.S. Foreign Service, he had worked in many facilities in similar shape throughout the world. He reported that it was difficult to move equipment around because the halls were only 36 inches wide and the elevator could hold only four passengers, never mind equipment. The only way to get some equipment moved was to manually haul it up and down the stairs. The embassy employee further stated he did not mind the rugged working conditions or long hours because he was accustomed to it from other embassy work. Every embassy was at the mercy of the host country because it had to depend on the host for water, electricity, and heat just as any other building in a country is dependent on that country for utilities. It was more difficult in Moscow because there was an adversarial relationship. Sometimes the Soviets played games by shutting off the utilities.¹⁴

The head of the State Department communication center at the Moscow embassy further described the atmosphere at the embassy as very intense. Nobody trusted the Soviets. He explained that workers took their jobs seriously. They were always under the watchful eye of the Soviets, even in their personal lives. He lived in an apartment outside the U.S. compound and would come home to find his freezer unplugged, shirts missing from his closet, or a dirty glass in the sink that had contained liquor. He was sure that the apartment had been bugged. Americans had no privacy.¹⁵

The replacement of all of the embassy electronic equipment had to occur with minimal impact on the mission. An NSA employee who was sent to the U.S. embassy in Moscow to carry out the replacement



Diplomatic pouches from the U.S. embassy in Moscow
await inspection in an NSA trailer

of the equipment explained that he arrived late on a Saturday and began working early on Sunday morning. He had two kinds of tasks: protect the equipment that was held overnight in the attic and help with the unloading and loading of equipment. He brought alarms and sensors that he set up in the attic. He ran the wires down to the Marine guards on the sixth floor. No one interfered with the equipment while NSA personnel were there.

According to him, the logistics of the operation were handled superbly, and a shipping clerk was part of the team. He opened the diplomatic pouch, uncrated the equipment, and opened the box. Everyone carried the equipment down to its position. While members of the team set up the new piece of equipment, others brought the old one back to the attic where it was repackaged in the box that had contained the new equipment. They spent lots of time running up and down the stairs. The teletype machines, in particular, were extremely heavy. They were also very wide and could barely fit through the stairways. He and his colleagues started changing equipment in the State Department communication center and sys-

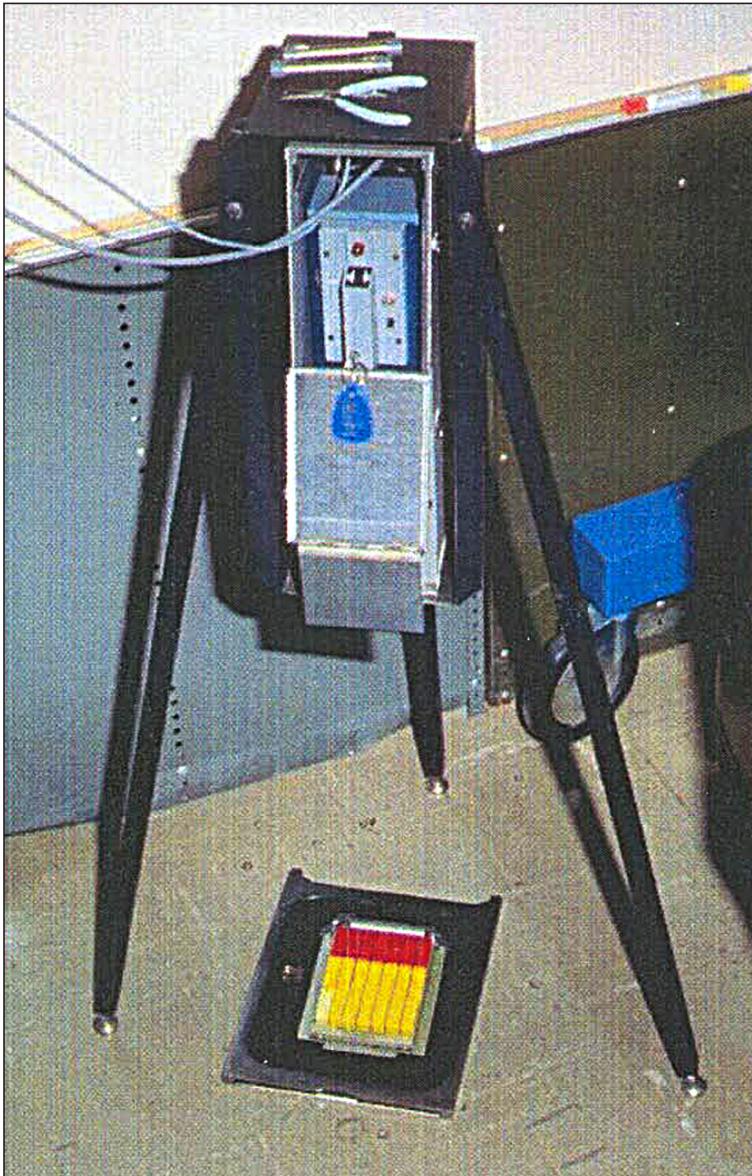
tematically worked their way through the rest of the building. He was at the embassy for 10 days for what turned out to be a “glorious adventure.”¹⁶

The Discovery

Since S65 handled a wide variety of special projects, it was appropriate to give this division the lead in looking for bugs in the U.S. embassy equipment. The head of this division reported that he pulled together a team of the best minds to work on this challenging task. This assignment was an unusual one for NSA. The division chief was careful to assign the right number of people because he did not want them getting in each other's way. They needed space to do their work. Too many people would have created confusion. He did not want them to inadvertently miss anything.¹⁷

As the equipment from the embassy was returned to NSA, the COMSEC organization began a lengthy inspection process of each item. The equipment had to be inspected methodically to prevent the destruction of important evidence. The accountable COMSEC equipment was examined in the labs inside the OPS3 or S building, the COMSEC facility on Fort Meade, while the nonaccountable COMSEC equipment was stored and examined in the trailers. Each item was inspected visually and then x-rayed. The x-rays were compared with known standards for each item.¹⁸

In describing the atmosphere as the search for bugs proceeded at NSA, an S65 physicist said the adrenalin was really flowing. About 25 people were involved in the search. They all recognized the importance of their work. NSA's reputation was on the line, and it was up to them to find something. They felt sure that the Soviets were taking advantage of the Americans. They worked six days a week and did not complain about rough working conditions. When



Primary x-ray machine used in detecting equipment bugs. This portable machine measured about $8 \times 6 \times 12\text{--}15$ in. It was pointed at the floor when taking an x-ray; a sheet of x-ray film was placed under the item.

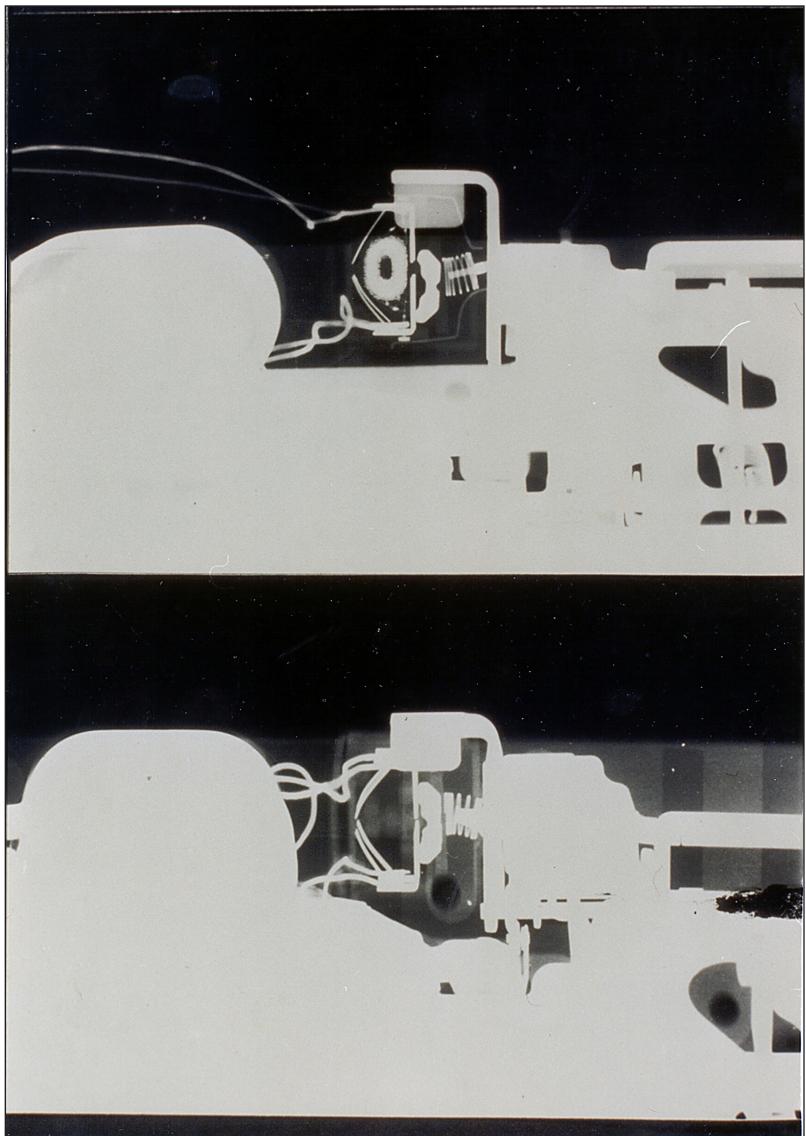


X-rays of equipment drying in an NSA trailer

they started working in the trailers, there were no steps up to the entrances, which were about four feet off the ground. They found some cinder blocks and empty spools that had contained mesh wire to help them enter the trailers. Eventually they got steps, phones, and air conditioning—and life improved.¹⁹

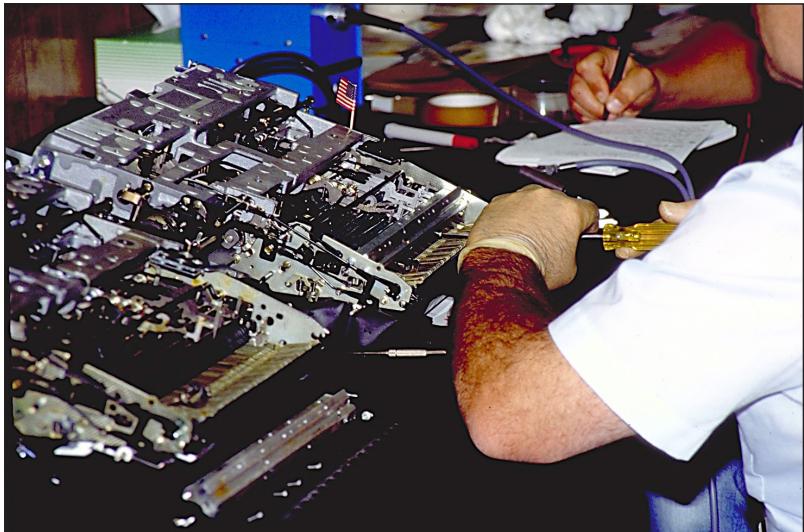
Walter Deeley had a long, varied career at the Agency. He had a reputation for being strong willed and abrasive, but committed to the mission. Directors of the Agency turned to him when they needed someone to accomplish a difficult job. As the head of the COMSEC organization, Deeley wanted the question of whether the Soviets were bugging U.S. equipment answered quickly. He demonstrated his impatience by swapping managers for the project in midstream.²⁰ He also offered a \$5,000 bonus to the person who found a bug.²¹

An engineering technician in S65 who was working on this project enjoyed the challenge of searching for a bug in the U.S. equipment. According to him, the 1980s were a time when people felt patriotism and pride in their country. They knew who the enemy was and wanted to limit the enemy's effect. The engineering tech



X-rays of rear of U.S. embassy typewriter

frequently worked at night and on the weekends by himself in the trailer, examining equipment. After he and his colleagues had looked at all of the cryptographic gear, they eventually made their way to



NSA engineers disassembling an embassy typewriter to search for bug; note the small flag they stuck in the housing

examining the typewriters. He took a typewriter apart to look at all of the possible places where a bug could be inserted. He created an image of these areas, which enabled him to take fewer but clearer x-rays of the important sections.²²

On a Monday evening, 23 July 1984, the engineering technician noticed an extra coil on the power switch of an IBM Selectric typewriter. He decided to x-ray the whole machine from top to bottom. The x-rays of the keyboard proved to be very interesting.²³ When he saw those x-rays, his response was “holy f***.” The Russians really were bugging the equipment. He was very excited, but no one was around to hear the news. Although his wife was an NSA employee, he could not tell her because of the level of classification for the project. He hardly could wait for morning when his colleagues would return.²⁴

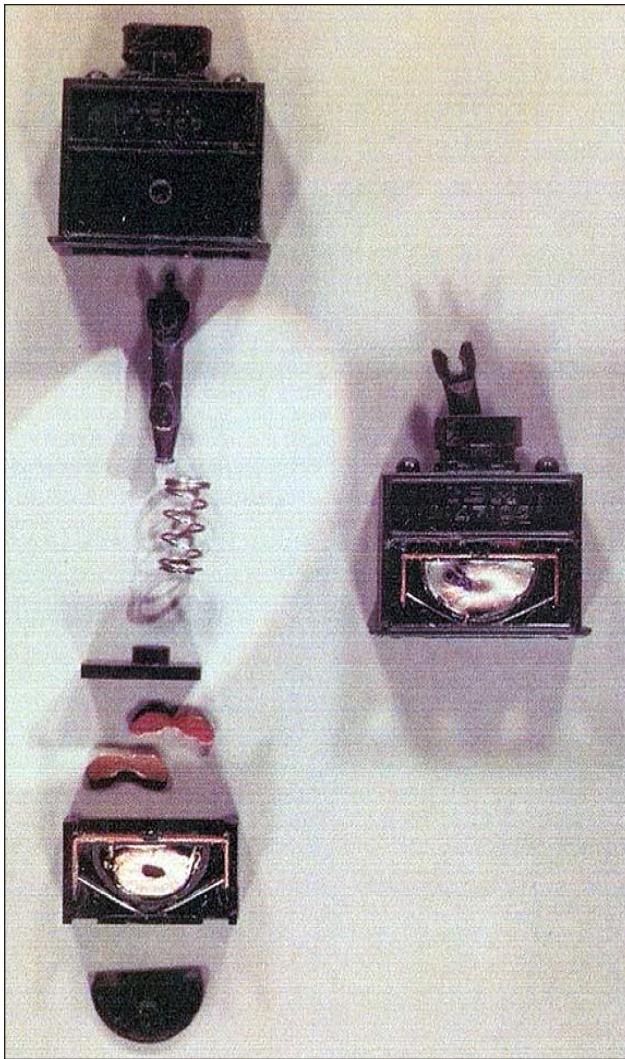
Another analyst explained that the next morning engineers argued about whether they had an anomaly or a bugged typewriter. Some typewriters had memory that could account for additional

circuits. What led them to conclude that this typewriter was probably bugged was the location of so many circuits in a metal bar that ran along the length of the machine. When their boss arrived, they informed him and he called in other experts from R9. Deeley shared the discovery with DIRNSA. Now the pace of work really increased.

NSA analysts had to thoroughly examine all other embassy typewriters in the USSR because most likely there were more bugs. They also had to educate other U.S. embassy personnel from Eastern Bloc countries on how to search for bugs. They likewise began the difficult task of reverse engineering the bug to see how it worked. One analyst had been discouraging the wide use of x-rays because the organization had difficulty obtaining Polaroid film. At that time, Polaroid made only about 3,000 sheets of film a year. They already had used 10,000 sheets and were having trouble getting more; however, there was no way to see the bug without x-rays.²⁵

The technician who discovered the implant claimed to have no special talent. He said that he found the bug by luck. After looking at so many x-rays day after day for so many hours, he could easily have missed it. He was glad that he saw it and certainly was delighted with the \$5,000 cash award.²⁶

Another technician believed that the GUNMAN experience had an important positive effect on the COMSEC organization since it taught them to expand their thinking. Many of those working in the COMSEC area expected the bug to be in cryptographic or other COMSEC equipment. It ended up being in a typewriter that produced plaintext. They would need to pay more attention to plaintext communication devices if they were to keep U.S. communications secure.²⁷



Exploded view of bugged power switch from a
U.S. embassy typewriter

Reactions to the GUNMAN Find

One technician characterized the reaction to the GUNMAN find within the organizations that had worked on the project as chaotic. He indicated that everyone jumped on the bandwagon and wanted to take credit for the discovery. He suggested that everyone wanted to be on stage, and S65 was pushed into the background. Deeley had handpicked the people to brief President Reagan at the White House. R9 grabbed the publicity, too.²⁸ As Count Galeazzo Ciano summed up human nature in his diary in World War II, “As always, victory finds a hundred fathers but defeat is an orphan.”

The discovery that the Soviets had bugged a typewriter in the U.S. embassy in Moscow did not diminish the level of secrecy surrounding the GUNMAN project. A technical writer in S64, the TEMPEST office,²⁹ which was located next to S65, saw large amounts of equipment going up and down the hall. She even helped with the procurement of film and packaging materials. She learned about the true nature of the GUNMAN project only after the implant was discovered. Even then her supervisor swore her to secrecy.

One morning, with no time for preparation, she was told to brief the deputy director, Robert Rich, on the GUNMAN implant. She did the best she could with the briefing, but determined that she would learn as much as possible about the subject. Since the engineers were very busy with their investigations, she soon became the NSA GUNMAN briefer.

While the search for additional bugs continued, the secrecy of GUNMAN remained paramount. The technical writer briefed Agency seniors about GUNMAN. People were briefed one at a time in an anechoic chamber, a soundproof anti-echo room used to conduct technical tests. She reported that the reaction to the news ranged from astonishment to anger.

Over time, the need to warn others of the Soviet threat grew, and NSA began to brief members of the Intelligence Community. Balancing the need for secrecy versus the need to warn against a threat was a difficult task. The technical writer briefed the GUNMAN project for seven years. One of the highlights for her was briefing the President's Foreign Intelligence Advisory Board. Normally this task would fall to Agency seniors, but none were available so she was able to go to the White House to make the presentation.³⁰ Other analysts who also worked in S64 reported that a GUNMAN briefing team went on the road to warn U.S. allies of the Soviet threat. Some team members gave presentations and some answered technical questions from the audience.³¹

In 1985, when the story of the Soviet bugging of U.S. typewriters in the Moscow embassy broke on the *CBS Nightly News*, William Casey, then CIA director, was furious. He demanded a list of everyone that NSA had briefed on the GUNMAN project. The technical writer was glad that she was able to supply that list. Casey eventually dropped the investigation of the leak because the task of discovery was impossible. Too many people knew about GUNMAN.³²

Implant Characteristics

A discussion arose within the COMSEC organization about whether the GUNMAN bug should be reverse engineered by a contractor or by the organization itself. Some engineers insisted that they had the capability to do this work. One had gained reverse engineering experience at a previous job with Naval Intelligence.³³ Management sided with the engineers, and reverse engineering of the GUNMAN bug became an in-house project. This was an important decision because it enabled NSA to learn a great deal about the ingenuity of the Soviets and to gain a better understanding of the threat. This decision also showed that management and subordinates had a good working relationship and that subordinates had initiative. It was an atmosphere that furthered the Agency's ability to fully carry out its mission.

NSA analysts left no stone unturned in reverse engineering the implant. The COMSEC and Research organizations devoted considerable time and effort to studying all aspects of the bug. NSA was determined to learn from the enemy. As the following discussion demonstrates, reverse engineering was very successful, and the analysts uncovered numerous characteristics of the implant.

A brief explanation of the general characteristics of IBM Selectric typewriters will aid in the understanding of how the implant worked. Most typewriters had metal arms that swung up against an inked ribbon to type a letter. IBM Selectrics, however, were unique because they used a round ball with numbers and letters embossed around the outside surface. When a typist struck a key, the ball

moved into position over an inked plastic ribbon and descended to imprint the character onto the paper.

The lot of equipment from the U.S. embassy in Moscow that was shipped back to NSA contained forty-four typewriters, six of which were bugged. The first step in evaluating the implant was to compare a bugged typewriter with a nonbugged typewriter. As S65 and R9 personnel disassembled the typewriters side by side, they took video and still photography of each part to ensure a thorough evaluation. Some of the unique characteristics of bugged typewriters were that these units had an additional spring lug and screw; a modified switch; and modified bails or arms that controlled the pitch and rotation of the ball. (The official term for bail is interpose latch.)



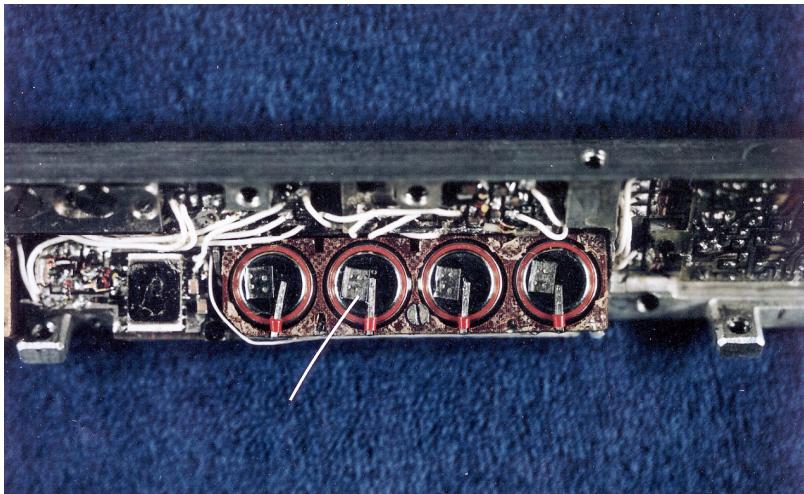
IBM Selectric typeball

Personnel from S65 and R9 divided the reverse engineering tasks. R9 personnel focused on the operational aspects of the bug. S65 personnel removed the printed wire assemblies and determined the emanation capabilities. Together, S65 and R9 personnel drew logic diagrams describing the circuits. S65 personnel also trained people from other agencies to perform visual and x-ray inspections of equipment in the field so that they could look for bugs. This training paid off because seven additional typewriters in the Moscow embassy and three typewriters in the Leningrad consulate contained implants. A total of sixteen bugs were found in twelve IBM Selectric II typewriters and four IBM Selectric III typewriters. Common features were found in all sixteen typewriters: six ferromagnetic magnetizable bails were replaced with six nonferromagnetic, nonmagnetizable bails with a very strong magnet in the tip; all the typewriters contained a modified comb support bar that housed the bug; and all used burst transmissions at the 30, 60, or 90 MHZ range via radio frequency.

The Soviets continually upgraded and improved their implants. There were five varieties or generations of bugs. Three types of units operated using direct current (battery) power and contained either eight, nine, or ten batteries. The other two types operated from alternating current (AC) power and had beacons to indicate whether the typewriter was turned on or off. Some of the units also had a modified on-and-off switch with a transformer, while others had a special coaxial screw with a spring and lug. The modified switch sent power to the implant. Since the battery-powered machines had their own internal source of power, the modified switch was not necessary. The special coaxial screw with a spring and lug connected the implant to the typewriter linkage, and this linkage was used as an antenna to transmit the information as it was being typed.³⁴ Later battery-powered implants had a test point underneath an end screw. By removing the screw and inserting a probe, an individual could easily read battery voltage to see if the batteries were still active.

The ingenuity of the Soviets was remarkable because their bugs did not merely move from batteries as a source of power to AC. There were early versions and later versions of bugs that used both sources of power. NSA found that the first three implants were battery powered. The first of these was shipped to Moscow in October 1976, and the other two were shipped in April of 1977. The first bug that used AC as its source of power was shipped to Moscow in November 1977. The remaining nine machines that were found in Moscow used AC as their source of power and were more advanced than the first AC-powered bug. Five of the advanced model AC bugged typewriters were delivered to Moscow in February 1982. The remainder were delivered in January of 1984.³⁵ The later battery-powered bugged typewriters found in the consulate in Leningrad were shipped in April of 1977 and March of 1982.³⁶

All of the implants were quite sophisticated. Each implant had a magnetometer that converted the mechanical energy of key strokes into local magnetic disturbances. The electronics package in the implant responded to these disturbances, categorized the underlying data, and transmitted the results to a nearby listening post. Data were transmitted via radio frequency. The implant was enabled by



Battery-powered implant, one of the five generations of bug types found in U.S. embassy typewriters

remote control.³⁷ Another advantage of these bugs was easy installation. Engineers estimated that a skilled technician could install an implant in a typewriter in a half-hour.³⁸ The integrated circuits were very sophisticated for that time period. The circuits contained one bit core memory, an advancement that NSA engineers had never seen.³⁹

When the press learned in 1985 that the Soviets were bugging typewriters in the U.S. embassy, reporters tried to describe the characteristics of these bugs. One of the more technical explanations appeared in the June 1985 edition of *Discover* magazine. How accurate was that description?

In an article titled “Tapping the Keys,” a bugging expert offered the following explanation of the Soviet bug:

The Soviets must have taken advantage of the way the Selectric types. A metal ball covered with characters spins so that the appropriate character strikes the paper and then spins back to its starting point. The time it takes to accomplish the rotation to each letter is different. A low-tech listening device planted in the room could transmit the sounds of a

typing Selectric to a computer. The computer could then easily measure the time intervals between each key stroke and the character being put on the paper, and thus determine which character had been tapped.⁴⁰

An engineer in the COMSEC organization who was involved in reverse engineering the GUNMAN bug explained that the press had a good idea, but it was inaccurate. While IBM Selectric typewriters used a spinning ball to get the right character on the paper, the bug was not based on sound or timing. He further elaborated that the Soviets were very good with metal, and housing the bug in a metal bar was ingenious. The bar was difficult to open and it concealed the bug from inspection.⁴¹ Another engineer from R9 who also worked on this project agreed. He noted that to the naked eye, the bar looked like a single unit. He could not see that it could be opened. The use of low power and short transmission bursts also made it difficult to detect this bug, which contained integrated circuits that were very advanced for that time. The Soviets had developed a very sophisticated implant.⁴²

The discovery of this bug by NSA technicians was a significant technical achievement.

The press did not understand the level of sophistication of the GUNMAN bug. For instance, an article from *Time* magazine speculated, “the Soviets somehow encoded the machine’s typing function, giving each character a distinguishing electronic or magnetic signature.”⁴³

In reality, the movement of the bails determined which character had been typed because each character had a unique binary movement corresponding to the bails. The magnetic energy picked up by the sensors in the bar was converted into a digital electrical signal. The signals were compressed into a four-bit frequency select word. The bug was able to store up to eight four-bit characters. When the buffer was full, a transmitter in the bar sent the information out to Soviet sensors.

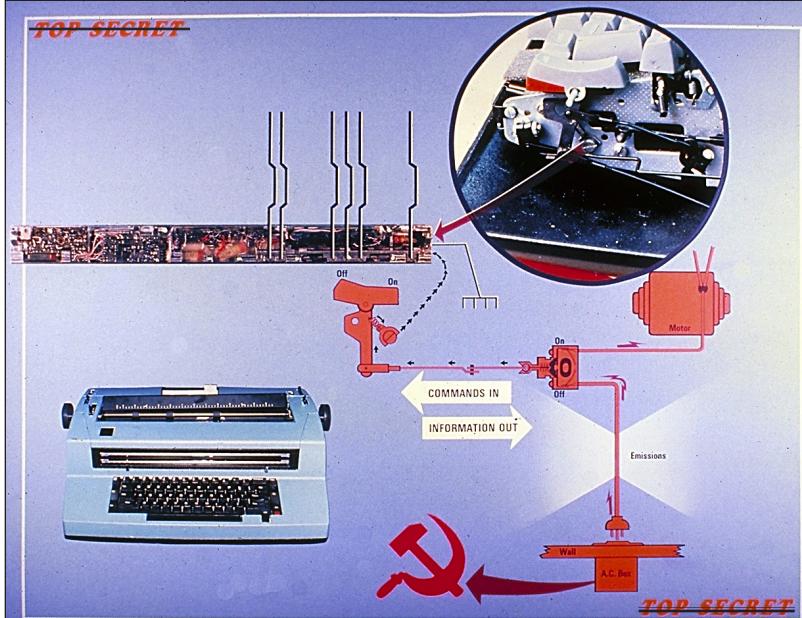
There was some ambiguity in determining which characters had been typed. NSA analysts using the laws of probability were able to figure out how the Soviets probably recovered text. Other factors that made it difficult to recover text included:

- The implant could not detect characters that were typed without the ball moving. If the typist pressed space, tab shift, or backspace, these characters were invisible to the implant.
- Since the ball did not move or tilt when the typist pressed hyphen (because it was located at the ball's home position), the bug could not read this character either.⁴⁴

Damage Assessment: A Cunning Enemy

Despite the ambiguities in knowing some of the typed characters, the typewriter attack against the United States was a lucrative source of information for the Soviets. It was difficult to quantify the damage to the United States from this exploitation because it went on for approximately eight years. The Federal Bureau of Investigation (FBI) examined typewriter inventory records to determine when the sixteen bugged machines arrived at the Moscow embassy and the Leningrad consulate, where the typewriters were located in each facility, and to whom they were assigned. The FBI was unable to uncover the answers to these questions for several reasons. The State Department had a policy at both the embassy and consulate levels of routinely destroying records every two years. State Department personnel normally rotated to new assignments every two years, so responsibility for procurement of typewriters and inventory controls and maintenance changed frequently. There was no continuity of procedures for inventory control.⁴⁵

Why did the United States fail to detect bugs in its typewriters for so long? One of the main reasons the bugs remained undetected for approximately eight years was that the United States used outdated and inappropriate techniques and equipment when conducting inspections and made mistakes in analysis. Another important reason was that the Soviets proved to be a cunning enemy. Much of the equipment used by U.S. Technical Security Countermeasure (TSCM) teams dated back to the 1950s. The GUNMAN device used burst transmissions that were so short the signal disappeared



A slide prepared for a briefing depicts
the GUNMAN discoveries

from the spectrum before it could be recognized by the older spectrum analyzers used by the TSCM teams. Burst transmissions also occurred intermittently due to the speed of the typist. Since the devices were remotely controlled, the Soviets could turn them off when inspection teams were in the area. Newer spectrum analyzers had memory and could integrate energy detected over a period of time. These newer analyzers may have detected the GUNMAN device, but there would have to have been an element of luck. While the spectrum analyzer was in use, the typewriter and bug would have to have been turned on and the analyzer tuned to the right frequency range.

The design of the GUNMAN bar indicated that the Soviets had knowledge of techniques used by American TSCM teams when inspecting facilities. For instance, the Soviets must have known that the Americans used nonlinear detectors because the GUNMAN device was designed to filter out frequency harmonics, which is an

integral part of what a nonlinear detector searches for. The Soviets also used “snuggling” techniques to hide the transmission of the bug in the noise of the transmission of television stations. They deliberately set the devices in the same frequency band as their television stations so that U.S. analyzers would miss the transmissions.

Once the GUNMAN bug was discovered, it became clear that some U.S. analysts had misinterpreted clues over the years. In 1978, inspectors found an antenna in the chimney in the U.S. embassy in Moscow. The Intelligence Community was never able to figure out the purpose of that antenna. Typewriters were examined in 1978, but the technician did not find any bugs. The technician assumed that if a modification had been made to a typewriter, it would be in the power structure. Therefore, he only took x-rays of the start capacitor and switch and the motor. In 1978, the source of power for the implants was batteries, so no changes were made to the power structure of the typewriter. Technicians missed the bugs. Despite other indicators of Soviet exploitation of typewriters, the U.S. Department of State took no action to protect its typewriters.⁴⁶

The Soviets exercised great caution with their own electric typewriters. They prohibited their staff from using electric typewriters for classified information. Manual typewriters that were to be used for the processing of classified information were to be shipped from Moscow to other Soviet embassies only in diplomatic pouches. When these typewriters were not in use at the various embassies, they were to be stored in sealed containers.⁴⁷

Some consolation from the U.S. perspective was that there was no indication that a U.S. person was involved in the GUNMAN attack. The implant devices most likely were installed by the Soviet intelligence service when the typewriters were under the control of Soviet customs officials before they reached their destination at the embassy or consulate.⁴⁸ NSA conducted investigations in U.S. embassies worldwide.⁴⁹ These facts do not diminish the ingenuity and determination of the Soviets.



Project GUNMAN exhibit at the
National Cryptologic Museum, Ft. Meade, MD,
showing the metal bar that concealed the typewriter bug

As General Faurer explained in 1986:

I think people tend to fall into the trap of being disdainful too often of their adversaries. Recently, we tended to think that in technical matters we were ahead of the Soviet Union—for example in computers, aircraft engines, cars. In recent years, we have encountered surprise after surprise and are more respectful. Most folks would now concede that they have enormously narrowed the gap and have caught us in a number of places.⁵⁰

GUNMAN Impact

The GUNMAN project had a major impact on the Intelligence Community (IC) as a whole. It brought about a greater understanding of the thinking and operations in Soviet society. The IC became more aware of the hostile electronic threat against the United States as NSA briefed all levels of government to warn of the danger. NSA was not out to assess blame; it took the problem-solving approach.⁵¹

The State Department viewed embassy security as a “lower priority” than NSA did in part because “their job is to understand the relations, the culture of that country, and to spread goodwill.”⁵² When the GUNMAN story broke in the press, the State Department was forced to take security more seriously. The Bureau of Diplomatic Security of the U.S. State Department and its Diplomatic Security Service were established officially on 4 November 1985. This bureau’s purview covered all aspects of the security needs for the department, for its facilities at home and abroad, and for its employees and their families. The importance of the new organization was indicated by its head being an assistant secretary of state.⁵³

Numerous panels were formed to investigate not only how and why the Soviets were able to bug embassy typewriters, but also all areas of embassy security. These panels made numerous recommendations. In 1986, Congress came up with a \$35 million appropriation to the Director of Central Intelligence to improve embassy security. Only some recommendations were implemented due to a lack of cooperation between the various segments of the IC. The congressional com-

mittees on intelligence oversight threatened to reorganize the technical security countermeasures organizations within the various agencies to bring about coordination and reduce duplication of effort. To avoid this type of congressional action, the IC formed the Senior Interagency Group for Intelligence. This body attempted to get the agencies to work together, but they found it difficult to share information. The CIA and the FBI, however, did reorganize and upgrade their technical security organizations.⁵⁴

Project GUNMAN had a long-term positive effect on the State Department's policies and procedures for shipping plaintext processing equipment. In 1988, the State Department built a facility to inspect and package all plaintext processing equipment that is shipped overseas. The department also maintains a list of preferred items that will enhance security.⁵⁵ Many people believe that in comparison to the rest of the IC, the State Department has the best security measures today for protecting unclassified equipment that is shipped abroad.

GUNMAN also had some positive effects on NSA. As an engineer in the Research and Development organization during the time of GUNMAN explained, "Before 1984, the community did not believe [in] NSA and its abilities. As a result of the 1984 work on GUNMAN, the stature of NSA in terms of dealing with the embassy security community ... changed radically. We became the voice to listen to, and I'm very proud of that."⁵⁶

Plans that had been stalled were implemented because of Project GUNMAN. For instance, the National Security Council promulgated National Security Decision Directive 145. This directive, signed on 17 September 1984, made DIRNSA the national manager for telecommunications and automation information systems security.⁵⁷

After the GUNMAN revelations, several changes came about within the COMSEC organization at NSA. While the GUNMAN discovery was not the only cause for these changes, it certainly influenced their implementation. In 1985, the name of the COMSEC organization was changed to the Information Security (INFOSEC) organization.⁵⁸ *Information security* denoted an expansion of respon-

sibilities for the organization. The organization had more to protect than just the transmission of information. This name change also reflected the greater awareness of the need to protect plaintext information and the intention of the Deputy Director for Information Systems Security to place greater emphasis on the protection of plaintext. NSA management reorganized the INFOSEC organization to better handle its information security responsibilities. For instance, the organization became more involved in technical security countermeasures. The Technical Security Engineering Center, X3, created on 14 May 1986, became responsible for advanced technology development, fabrication security (the security of equipment as it is being built), technical security, and facility evaluation. Plans called for X3 and R9, which were responsible for the exploitation of the adversary's communications, to jointly conduct facility evaluations. NSA hoped to improve technical security through this more coordinated approach.⁵⁹

In the late 1970s, an expert from CIA came to NSA to start an anti-tamper technology program. In the spring of 1984, when NSA sent replacement equipment to the Moscow embassy, NSA had its own program to protect keying material and equipment, but it was small in comparison to the CIA program.

Because of the GUNMAN revelations and other intelligence compromises, such as the Walker spy ring,⁶⁰ NSA expanded its anti-tamper program. Customers were more receptive to using these solutions because they recognized the security threat. Technicians at NSA invented new anti-tamper technologies such as holograph and prism labels that could not be easily duplicated by an adversary who tried to remove them from a package.⁶¹

On 1 May 1989, in recognition of both the growth and importance of these technologies, the INFOSEC organization consolidated all of its anti-tamper programs into a new separate division, Y26, the Protective Technologies Implementation Division.⁶² In recognition of the need to train customers in the proper use of tamper technologies, a separate awareness and education branch was established within the division. Prior to the formation of this

branch, technologies were provided to the customer without any emphasis on their proper use. A chemist who worked in various technology tamper programs remembered a visit she made to see a customer on the USS *Mount Whitney* in the spring of 1984. When she asked the COMSEC custodian where he stored the keying material, he showed her the plastic bags that had contained a tamper-proof canister. He praised the use of the plastic bags and said they were great for storing fish bait. To her horror, the fellow was removing all of the keying material from the canister, which was intended for key storage, instead of removing only the key needed for that day. He completely eliminated the tamper protection. But, she noted, without training, what could NSA expect?⁶³

Corrective actions were taken and, because of its anti-tamper program, NSA became a leader in technical security.

Conclusions

From approximately 1976 to 1984, the Soviet Union used electromechanical implants to gather information from typewriters located in the U.S. embassy in Moscow and the U.S. consulate in Leningrad. Project GUNMAN was NSA's plan to first remove communications and information processing equipment from the U.S. embassy in Moscow and bring it back to Fort Meade. Phase two of the project was to thoroughly examine each piece of equipment in search of a bug. GUNMAN was well planned and well executed. Within five months, ten tons of equipment were procured and delivered to the embassy without interruption to embassy operations. Eleven tons of equipment were brought back to Fort Meade, and the first bug was discovered on 23 July 1984. NSA managers were able to move a large bureaucracy into action to meet a major threat to U.S. security. The actual discovery of the bug demonstrated the talent of NSA technicians.

Eight months after the GUNMAN discovery, the story broke in the press. By highlighting the damage, press coverage helped to focus the attention of the U.S. government on improving the security of its information. The press did not fully understand the level of sophistication of GUNMAN technology. They also did not appreciate the effort and talent used to discover the bug.

The GUNMAN experience had many positive effects on the Agency. NSA elements shared information and worked more cooperatively. The COMSEC organization gained a deeper appreciation of the ingenuity of the Soviets and thus a greater understanding of the

threat to U.S. communications. Project GUNMAN demonstrated that the Soviets could be extraordinarily innovative and technologically sophisticated in their efforts to gain intelligence from U.S. diplomatic facilities. More Agency personnel gained expertise in reverse engineering, and there was a greater appreciation of the benefits of these techniques. NSA placed increased emphasis on the development of anti-tamper solutions to protect equipment, and customers were more interested in using these technologies. NSA learned valuable lessons from the enemy.

As a result of Project GUNMAN, NSA gained a stronger reputation as an expert in technical security within the U.S. government. Consequently, NSA was called upon to evaluate facilities and to provide advice to other segments of the government.

The GUNMAN incident had the greatest impact on the Department of State. Because of the discovery of the typewriter bugs and other security problems, the State Department developed better security policies and procedures, especially in inspection and shipment of equipment.

GUNMAN did not have as much of an impact on the rest of the IC. Individual agencies upgraded their own technical security efforts, but there was only limited progress in working cooperatively or sharing information.

Project GUNMAN led to a great flurry of investigations in which the United States attempted to learn from the Soviets. The question was not did we learn from the enemy, but how long will the U.S. government and the IC remember the lessons that they learned from the GUNMAN project?

Although the GUNMAN discovery occurred decades ago and the Soviet Union was dissolved in 1991, the GUNMAN story is still relevant for the IC. Project GUNMAN illustrated what can happen when we underestimate the capabilities of an adversary. It also highlighted the need for vigilance in maintaining security.

Acknowledgments

I wish to acknowledge the men and women of NSA who graciously and enthusiastically described their experience with Project GUNMAN. I also appreciated their patience and willingness to explain technical details of the project. This publication would not have been possible without their assistance. I also wish to acknowledge the NSA Historian and the editorial staff of the Center for Cryptologic History for their guidance and assistance.

Notes

1. Transcript, *CBS Nightly News*, March 25, 1985.
2. George F. Kennan, *Memoirs: 1950 to 1963* (New York: Pantheon Books, 1972), 152-57.
3. Transcript, *CBS Nightly News*, March 25, 1985.
4. COMSEC Organization, NSA, “A Special Report to the U.S. Congress: Project GUNMAN,” March 1985, “Background,” NSA Archives, Accession 48399.
5. COMSEC Organization, NSA, “A Special Report.”
6. “Project GUNMAN: After the Smoke Cleared,” November 1986, 7-8, NSA Archives, Accession 46286.
7. Lt. Gen. Lincoln D. Faurer, USAF, interview by Tom Johnson, NSA-OH-1998-17, Center for Cryptologic History, Ft. Meade, MD.
8. Interview by Tom Johnson, NSA-OH-1996-34, Center for Cryptologic History, Ft. Meade, MD.
9. Interview by Tom Johnson, NSA-OH-1998-14, Center for Cryptologic History, Ft. Meade, MD.
10. “Project GUNMAN: After the Smoke Cleared,” 10-11.
11. S65 COMSEC Standards and Advanced Technology Division, “Evaluation of Project GUNMAN,” January 28, 1985, NSA Archives, Accession 49509.
12. COMSEC Organization, NSA, “A Special Report.”

13. Interview, NSA-OH-1998-14.
14. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2007-20, Center for Cryptologic History, Ft. Meade, MD.
15. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2007-29, Center for Cryptologic History, Ft. Meade, MD.
16. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2006-38, Center for Cryptologic History, Ft. Meade, MD.
17. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2007-06, Center for Cryptologic History, Ft. Meade, MD.
18. S65 COMSEC Standards and Advanced Technology Division, "Evaluation of Project GUNMAN."
19. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2006-17, Center for Cryptologic History, Ft. Meade, MD.
20. Discussion with the author, December 18, 2006.
21. Interview, NSA-OH-1998-14.
22. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2007-07, Center for Cryptologic History, Ft. Meade, MD.
23. Interview, NSA-OH-2006-17.
24. Interview, NSA-OH-2007-07.
25. Interview, NSA-OH-2006-17.
26. Interview, NSA-OH-2007-07.
27. Interview, NSA-OH-2006-17.
28. Interview, NSA-OH-2007-06.
29. TEMPEST is a codename referring to investigations and studies of compromising emanations. These are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.

30. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2006-09, Center for Cryptologic History, Ft. Meade, MD.
31. Interview by Tom Johnson, NSA-OH-1998-15, Center for Cryptologic History, Ft. Meade, MD.
32. Interview, NSA-OH-2006-09.
33. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2006-47, Center for Cryptologic History, Ft. Meade, MD.
34. S65 COMSEC Standards and Advanced Technology Division, “Evaluation of Project GUNMAN.”
35. “Twelfth Interim Analysis Report on the GUNMAN Find,” October 18, 1984.
36. “Thirteenth Interim Analysis Report on the GUNMAN Find,” October 25, 1984.
37. “Sixth Interim Analysis Report on the GUNMAN Find,” September 6, 1984.
38. “First Interim Analysis Report on the GUNMAN Find,” n.d.
39. Interview by David Cooley and Sharon Maneki, NSA-OH-2009-03, Center for Cryptologic History, Ft. Meade, MD.
40. “Tapping the Keys,” *Discover*, June 1985.
41. Interview, NSA-OH-2006-47.
42. Interview by David Cooley and Sharon Maneki, NSA-OH-2008-79, Center for Cryptologic History, Ft. Meade, MD.
43. “A Deadly Serious Game,” *Time*, April 8, 1985.
44. “GUNMAN Text Recovery from IBM Selectric III Typewriters,” C Expository Report No. 18-91, July 19, 1991, NSA Archives, Accession 49509.
45. “Parting Shot: Espionage Russia,” Federal Bureau of Investigation, March 15, 1985, 2, NSA Archives, Accession 49509.
46. “The Legacy of GUNMAN,” briefing to the NSA workforce, November 1, 2000, NSA Archives, Accession 49509.

47. "Project GUNMAN: After the Smoke Cleared," 19-21.
48. "Parting Shot: Espionage Russia," Federal Bureau of Investigation, 10.
49. "Project GUNMAN: After the Smoke Cleared," 40.
50. Ronald Kessler, *Moscow Station: How the KGB Penetrated the American Embassy* (New York: Macmillan, 1989), 97.
51. Interview, NSA-OH-1998-15.
52. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2006-34, Center for Cryptologic History, Ft. Meade, MD.
53. J. Craig Barker, *The Protection of Diplomatic Personnel* (Burlington, VT: Ashgate Publishing, 2006), 1-15.
54. "Project GUNMAN: After the Smoke Cleared," 23-25.
55. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2007-18.
56. Interview, NSA-OH-2006-38.
57. "Project GUNMAN: After the Smoke Cleared," 37.
58. Organization Audit Trail Database (OATS).
59. "Project GUNMAN: After the Smoke Cleared," 41.
60. In 1985, a spy ring consisting of former Navy personnel John Walker, Jerry Whitworth, Arthur Walker, and Michael Walker were convicted of (or pled guilty to) charges of passing classified U.S. intelligence material to the Soviet Union from 1968 to 1985. The ring reportedly helped the Soviets decipher more than one million encrypted U.S. naval messages.
61. Interview, NSA-OH-2006-17 (email attachment to transcript).
62. Organization Audit Trail Database (OATS).
63. Interview by Linda Murdock and Sharon Maneki, NSA-OH-2007-27, Center for Cryptologic History, Ft. Meade, MD.

