Cryptologic Almanac 50th Anniversary Series

VENONA: An Overview

(U) "Spy catching" is an alluring phrase more often connected with James Bond than with a cryptanalyst. However, during the Cold War, a group of cryptanalysts assisted the spy catchers in their efforts to stop Soviet espionage in the United States and other allied countries. Their decrypts revealed, among other things, the extent of the KGB operations in the United States and furthered the FBI's and other agencies' efforts in tracking down these spies.

(U) VENONA was the final in a series of cover names for the project to exploit cryptosystems used to protect what was initially believed to be Soviet diplomatic communications. The messages were encrypted using a complicated code that was then superenciphered by adding a numeric key stream from a one-time pad to the code. After some analysis, the cryptanalysts discovered they were really attacking five different systems being used by five different entities instead of one as originally thought. The five users for the five versions of VENONA were Soviet trade representatives, Soviet diplomats, and three Soviet spy agencies (the KGB, the Soviet Army General Staff Intelligence Directorate (GRU), and the Soviet Naval Intelligence, Staff (GRU-Naval)).

~~(TS//SI)~~ Although American cable companies, at the direction of the U.S. Army, had been collecting VENONA messages since 1939, there was no serious effort against the traffic until 1 February 1943. Prior to that time the system was believed unbreakable and thus not worth the cryptanalytic effort. One-time pads were and are still considered one of the most difficult manual cryptosystems to exploit; properly used, a one-time pad is virtually unbreakable. However, [redacted] inspired the American analysts to reexamine the traffic. (b)(1)

~~(TS//SI)~~ A team headed by a newly hired analyst named Gene Grabeel was assembled to study VENONA. The work was extremely difficult and went very slowly. In October 1943, Lieutenant Richard T. Hallock and his team, who were now also working on the project, identified clues that the additive key employed to superencipher the code may have been used more than once creating the condition known as a depth. Depth isolation was furthered in November 1944 by Genevieve Feinstein, who figured out that the Soviets were sending groups of key from the one-time pads in the messages in the clear, and if the same key group was found in the same correct position in two messages, these messages were in depth. As it turned out, the Soviet company that generated the KGB's one-time

pads produced about 35,000 pages of duplicate key as a result of pressures brought by the German advance on Moscow during World War II. The duplicate pages were sent to distant entities in an attempt to lessen the impact of this weakness. Although it was believed at that time that two deep depths were not exploitable, new techniques were invented by the cryptanalysts for this application. While it took another long period of hard work, many of the depths created by the manufacturing error were isolated and exploited. Once the additive key was stripped off, the monumental task of breaking the underlying code had to be completed before intelligence could be recovered. The gifted linguist Meredith Gardner led this effort and read the first message in February 1946. Slowly, over many years of work, the American cryptanalysts chipped away at the code and began to understand the underlying messages.

(U) This whole effort was made even more difficult by the fact that the Soviets disguised the identities of important people, places, and entities in the final text with code names. For example, KAPITAN was the code name for President Franklin D. Roosevelt; spy Elizabeth Bentley was GOOD GIRL; and San Francisco was called BABYLON. Because there were hundreds of code names used in the VENONA messages, this task was not a trivial one. Some code words were fairly obvious and appeared dozens of times. Others appeared only once or twice and to this day are unknown. From the context of the messages and additional outside information, the analysts were eventually able to identify many of the players and locations described in the messages. Not all the people referred to in the messages were spies. However, once identified, the code names fingered many of the Soviet spies operating in the United States.

~~(TS//SI)~~ Although only about 3,000 of the many thousands of VENONA messages sent from 1940 through 1948 were even partially read and translated, a surprisingly large amount of valuable information was recovered from those decrypts. Yet due to their classified nature, few people at the time ever knew the decrypts existed. The first message that grabbed the attention of the officials cleared for VENONA was one decrypted and translated in December 1946 that contained a list of names of American scientists working on the atomic bomb. Later messages revealed the identities and activities of several people passing atomic secrets to the Soviet Union, including Julius and Ethel Rosenberg, Harry Gold, David and Ruth Greenglass, and Klaus Fuchs. VENONA decrypts revealed general information about Soviet espionage activities in the United States as well as the identities of over 200 individuals connected with the GRU or KGB. Further, other decrypted messages helped paint a picture of the day-to-day business of Soviet espionage in the United States. Finally, VENONA allowed the U.S. to confirm the confessions of former spies, like Elizabeth Bentley, that were held in doubt until this evidence appeared. While the trade and foreign ministry messages were not considered of intelligence value and thus rarely translated, they were important because they helped the analysts break the ciphers on the KGB and GRU channels. It was the secret agent materials (KGB, GRU, and GRU-Naval) that proved the most valuable and exciting.

(U) It was because of such recovered information that FBI agent Robert Lamphere became the FBI liaison to the project in 1948. Due to the extreme secrecy of the project, VENONA decrypts could be used only to point investigations in the right direction; the FBI was forced to gather evidence to convict the Soviet spies from other sources. Yet, in spite of this limitation, this early cooperation between SIGINT and law enforcement agencies proved quite successful as demonstrated by the capture of spies like Julius and Ethel Rosenberg.

(U) At the request of NSA customers (FBI, CIA, and intelligence services of other allied countries) who hoped that additional spies might be identified, VENONA was worked until 1 October 1980. At that time, it was determined that the analysis of the VENONA traffic had been completed as much as possible. Also, it was decided that many of the spies discussed were probably no longer worth pursuing or possibly dead since the earliest traffic was now over forty years old. Yet, during the lifetime of the project, VENONA proved an extremely valuable weapon in the Cold War. It put numerous Soviet spies out of business either by arrest or by forcing them to flee to safety in another country as the FBI closed in. It also gave us a picture of what was really going on.

(U) Some argue that the fact that VENONA was broken is a miracle in itself. One-time pads are nearly impossible to break under the best of circumstances, and the successes against VENONA were accomplished without supercomputers, capture of keypads, or even a stolen codebook! It took a collection of gifted cryptanalysts to make the nearly impossible happen and break this system which proved so valuable in the spy game of the Cold War.

Sources:

(U//~~FOUO~~) Benson, Robert L., _The Venona Story_. Ft. George Meade, MD: Center for Cryptologic History, National Security Agency, 2001.

(U//~~FOUO~~) Benson, Robert Louis, and Cecil James Phillips. _History of VENONA_. Ft. George Meade, MD: National Security Agency, 1995.

(U//~~FOUO~~) Benson, Robert Louis, and Michael Warner, eds. _VENONA: Soviet Espionage and the American Response_. Washington, DC: National Security Agency and Central Intelligence Agency, 1996.

[(U//~~FOUO~~) Jill Frahm, Center for Cryptologic History, 972-2893s, jefrahm@nsa]

Horizontal Line