
From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 27 • NUMBER 1 • Winter-Spring 2022 $15 SINGLE COPY PRICE

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE, SUITE 324
FALLS CHURCH, VIRGINIA 22043
WEB: WWW.AFIO.COM * E-MAIL: AFIO@AFIO.COM

VENONA

by David Hatch

By shortly after the end of World War II, Soviet espionage had cleaned out the American safe: there were not many, if any, important US defense secrets that the Soviets had not accessed. During the war, the FBI had focused on German spies and sympathizers, and had stifled Nazi spying, sabotage, and subversion. However, at the same time, the Soviet Union, although a wartime ally of the United States, operated an extensive espionage network that obtained details on the development of military aircraft, radars, and other high-tech data, including atomic research. The Soviets also got political and diplomatic secrets, including inside information on the close US-UK relationship.

This hemorrhage of secrets was stopped in the early 1950s when the United States wielded one of the most powerful counterintelligence tools it had ever had. Ironically, the initial development of this tool was inadvertent.

Soon after the United States entered the war, Congress passed a censorship bill that addressed international telegrams.[1] Two copies of all cables sent and received from foreign countries had to be turned over to the censorship authorities; if a telegram was encrypted, one of the copies was forwarded to the Army's cryptologic organization.

During the war, the Soviet Union did not have its own international communications network, so it sent its diplomatic messages to and from the United States via commercial carrier such as Western Union. In accordance with international practice, all these Soviet communications were enciphered, therefore one copy went the Army's Signal Security Agency (SSA), headquartered at Arlington Hall Station in northern Virginia.[2]

In the middle of the war, as American policymakers became worried about the Soviet Union's plans related to Japan, with which the USSR had a neutrality pact,[3] Military Intelligence asked the SSA to look into those enciphered Soviet telegrams. Since the SSA had had good success against ciphers used by the Axis powers and many neutral nations, this seemed a way to get accurate information about Soviet future policy. However, despite their professional skills, the cryptanalysts at Arlington Hall decided that the Soviet communications could not be exploited – they had been encrypted by a one-time pad system, a type of encryption that could not be solved.

After the surrender of the Axis powers in 1945, American cryptanalysts no longer had urgent targets, so they began to study a variety of foreign communications with a view to expanding their knowledge of the science of cryptology. Among the systems studied were the wartime Soviet diplomatic messages that had been put aside as unsolvable. In this re-examination, analysts discovered statistical anomalies that would not be present in a true one-time pad system. This raised the hope that these messages might be solved after all.

The Army Security Agency (ASA), the successor to the SSA, put together a team of analysts, led by Genevieve Grotjian, who had made important breakthroughs against Japanese systems, and including Cecil Phillips, a future senior leader at the National Security Agency. The team discovered the Soviets had committed a major blunder in encrypting these diplomatic messages. For reasons unknown, probably due to wartime pressures as German armies approached Moscow, the Soviets had used some pages of their one-time pads twice! They had been clever about how they distributed these duplicate pages, so it was not apparent to any of their own users, but this critical mistake was discovered by the American analysts.

Even two-time use of a one-time pad did not ensure that the underlying message could be recovered. American analysts had to develop new statis-

1. Executive Order 8985, dated December 19, 1941, established the Office of Censorship that had "absolute discretion" over censoring international communications. *https://en.wikipedia.org/wiki/Office_of_Censorship*

2. The SSA was renamed as the Army Security Agency (ASA) in 1945 and later absorbed into the Army's Intelligence and Security Command (INSCOM) in 1977. *https://www.army.mil/inscom/?-from=org#org-history*.

3. Despite being allies US-Soviet relations were often strained during World War II. When the Normandy invasion was postponed again in early 1944 Stalin recalled the Soviet ambassadors in London and Washington raising fears that Moscow might seek a separate peace with the Nazis and alter the alliance in other ways. "US-Soviet Alliance, 1941-1945," Office of the Historian, US Department of State. *https://history.state.gov/milestones/1937-1945/us-soviet*.

tical techniques to exploit the messages. A team led by Meredith Gardner, a polyglot who was what NSA today calls a "cryptolinguist," made progress against a number of the messages. They began to recover words in the places where the Soviets had misused the one-time pads, although much of the text remained unintelligible.

As more code recoveries were made and further analysis done on the communications patterns, Arlington Hall analysts concluded that this system had five users: Soviet diplomatic network, an office tracking American lend lease goods to the Soviet Union, but also the KGB,[4] Soviet military intelligence, and a Naval intelligence organization. Moreover, many of the messages had significant clues to the identity of Americans providing the Soviet Union with classified information.

As more complete passages became intelligible, sometimes to include entire messages, the ASA faced a dilemma. The Agency was now in possession of extremely important information about Soviet espionage in North America, but neither the ASA nor the Army could make use of it. Under the 19th century Posse Comitatus law the US military was barred from engaging in law enforcement activities in the United States.

Therefore, the Army's leadership decided it was necessary to share this information with the FBI. But there was an important stipulation. The FBI had to agree that the fact that these messages had been solved could not be made public, nor could they ever be used as evidence in court. Essentially, the FBI had to use them as "starter kits" to direct investigations that would develop evidence that could be used in open court.

J. Edgar Hoover agreed to this condition, and assigned a veteran counterintelligence investigator to work with Arlington Hall to make use of this serendipitous find. As the investigator, Robert Lamphere, later wrote,

> *"I stood in the vestibule of the enemy's house, having entered by stealth I held in my hand a set of keys.... I had no idea where the corridors of the KGB edifice would take us... but the keys were ours, and we were determined to use them."*[5]

This effort against Soviet espionage communications remained top secret until 1995. In the early days, it had several designations, but it is best known by its long-term cover name, project VENONA.

The messages being exploited were primarily wartime communications, most fell within the 1941 to 1946 timeframe. In the end, only a very small percentage of the total Soviet message traffic was exploited – out of approximately 8,000 KGB messages sent in this time period, only about 2,000 were exploited; out of about 7,000 messages from Soviet military intelligence, only about 500 would be solved. But, despite the age of the messages and the low ratio that were solved, from a counterintelligence standpoint, the VENONA messages were pure gold.

What did this inside look at KGB operations reveal?

The messages revealed a good deal about espionage tradecraft in recruiting and handling Americans who had access to sensitive information. The messages included cover names for the Americans who were providing them secrets, but many messages describing the type of information involved and the kinds of access the American informants had provided clues that allowed the FBI to identify the US contacts who had violated their loyalty oaths.

A Sample of Cover Names
discovered in Venona decrypts

VICTOR — LTG Pavel Fitin (VENONA messages were signed or addressed VICTOR)
KAPITAN — President Roosevelt
BOAR — Winston Churchill
FELLOWCOUNTRYMAN — Any member of the Communist Party of the USA
ANTENNA (later LIBERAL) — Julius Rosenberg
BABYLON — San Francisco
CARTHAGE — Washington, D.C.
ARSENAL — US War Department
THE BANK — US State Department
HUT — OSS
ENORMOZ — The Manhattan A-Bomb project
ANTON — Leonid Kvasnikov (KGB chief of A-Bomb espionage in New York)

One of the first KGB contacts identified through analysis of the VENONA material was Judith Coplon, an employee of the Justice Department. Although the Justice Department kept her under surveillance for some time, they did not discover any evidence of disloyalty. So, they set up a sting. They concocted a false but credible document, placed a classification

4. For ease of understanding, "KGB" is used throughout this article to signify the USSR's secret service. It was known as the NKVD from 1934 to 1941, and after several name changes in 1954 became the well-known KGB. See Robert W. Pringle, *Komitet Gosudarstvennoy Bezopasnosti*, *https://www.britannica.com/topic/KGB*.

5. Robert Lamphere, *The FBI-KGB War: A Special Agent's Story* (New York: Random House, 1986), p. 86.

Prominent Soviet Sources Revealed in Venona Decrypts		
Name	**Position**	**What S/He Revealed to Soviets**
Julius Rosenberg	Private citizen, with contacts among electrical engineers working for the government	Data about US fire control systems, radar, and technical developments in the Army Signal Corps.
David Greenglass	Enlisted man, Los Alamos	Machining the shell for the atomic bombs.
Klaus Fuchs	British scientist at Los Alamos	Theoretical physics behind the atomic bomb.
Judith Coplon	Employee, Justice Dept.	Justice Dept policies and cases regarding foreign agents.
Harry Dexter White (died before indictment)	Senior official, Treasury Department	U.S. monetary policy during WWII.
Guy Burgess & Donald McLean	Members of the UK diplomatic service	Developments and issues in the US-UK wartime alliance.
Source: Robert Benson. The Venona Story, Center for Cryptologic History, National Security Agency, https://www.nsa.gov/Portals/70/documents/about/cryptologic-heritage/historical-figures-publications/publications/coldwar/venona_story.pdf		

on it, then dangled it in front of Ms. Coplon. The FBI arrested her on March 4, 1949, as she was passing what she thought was classified information to a Russian employee of the United Nations in New York City.

Elizabeth Bentley had been a courier for the KGB, collecting government documents from a number of individuals and passing them to KGB officers. The Soviets however, considered her unreliable and dropped her. Angry, Ms. Bentley, beginning in early November 1945, told the FBI all she knew about Soviet espionage in the United States and about the Americans who had passed her classified information. She was never told about VENONA, but she was considered a reliable source by the FBI because much of what she said about disloyal Americans was confirmed in VENONA decrypts.

VENONA decrypts led the FBI to a variety of government employees at many levels. Among those whose undercover activities were exposed in the decrypts were Harry Dexter White, a senior official in the Treasury Department; Alger Hiss, a senior policy official in the State Department; Duncan Lee, who had been a senior officer in the OSS; and Laughlin Currie, who had been an important aide to President Roosevelt in the White House. In addition to government officials, according to VENONA, scientists working on the MANHATTAN project in World War II had given the KGB information, as had several employees with access to high-tech industrial secrets.

The VENONA decrypts contained the initial clues and eventually details about the most controversial espionage ring in American history, that of Julius and Ethel Rosenberg. Early decrypts revealed many of the actions Rosenberg took to acquire classified information on American weapons development during the war; decrypts also revealed that he had persuaded his brother-in-law, a machinist working on the atomic bomb at Los Alamos, New Mexico, to tell what he knew about the bomb to Soviet officers. Eventually, the decrypts provided sufficient personal information to allow the FBI to identify the Rosenbergs and Ethel's brother, David Greenglass. The Rosenberg case was controversial in its time and continues to be controversial today. It is true that much of the evidence presented at their trial seemed sketchy, but, behind-the-scenes, the government knew full well that the husband and wife were guilty.

It is apparent that the Soviets knew about the breakthrough into the VENONA messages almost from the start. William Weisband, a Russian linguist working for the Army's cryptologic organization, and Harold A. R. "Kim" Philby, the British liaison officer to the American intelligence community, both knew about the project, and apparently told the Soviets all they knew. However, the Soviets could not retrieve the messages that the US had and probably did not know the extent of American exploitation of them.

Project VENONA continued until 1980, with analysts still working on messages from the Second World War. By 1980, however, senior officials at NSA recognized that while some additional information might be gleaned from messages yet unsolved, it was unlikely the cost of continuing to keep the project active would produce enough results to justify the expense.

Despite the high classification on the project, even after it was put in inactive status, rumors about its existence and who the messages implicated circulated throughout the national defense community and probably the academic world as well. In the early 1990s, Robert Lamphere, one of the original FBI

Significant VENONA Personalities

Lt. Leonard Zubko: A graduate of Rutgers University in mechanical engineering, Lt. Zubko had grown up bilingual in English and Russian. Assigned to Arlington Hall Station in 1943 and tasked with beginning analysis of the VENONA traffic, Lt. Zubko did not take to cryptologic work and was reassigned to a combat support unit at his request. After the war he had a career in aeronautical engineering.

Gene Grabeel: A schoolteacher from southwestern Virginia, Gene Grabeel wanted to do something to help war effort, and was recruited for work at Arlington Hall in 1942. She began the analysis on the VENONA traffic in 1943 and spent her entire career on the Venona analytic problem, retiring in 1980.

Genevieve Grotjean: A statistician in another government department, she was recruited by Arlington Hall in the late 1930s. Before World War II, she made the initial findings that enabled solution of the Japanese diplomatic cipher system known to the Americans as PURPLE. She resigned from the Army's cryptologic organization shortly after the war, become a housewife and mother.

Cecil Philips: He was a college student as America entered the war, but was rejected for service because of a minor physical disability. He sought a civilian job and was assigned to Arlington Hall. His analytic skills were important in uncovering the Soviet misuse of one-time pads in the VENONA traffic. After the war, he rose to senior positions at NSA, and became a major figure in the early computerization of cryptologic work.

Meredith Gardner: He was a multi-linguist, and was initially hired by Arlington Hall because of his knowledge of German. During the war, he also learned Japanese to help in cryptanalysis, and at the end of the war, studied Russian. He spent his entire postwar career doing cryptolinguistic analysis of the VENONA traffic.

investigators into the decrypts, wanted to publish his memoirs, but was denied permission to read the VENONA documents on the grounds of their continued high classification level. However, in 1995, NSA, in response to appeals of freedom of information act denials for release of VENONA decrypts, decided it was time to release all of them.

NSA proceeded to do this in stages over the next year, starting with the decrypts relating to espionage against the MANHATTAN project, which included the Rosenberg material. Today, all the VENONA decrypts may be read at www.nsa.gov, along with a number of analytic documents written by Meredith Gardner and other analysts.

In the 1980s, when NSA released the ULTRA decrypts from World War II, the new information caused historians to re-evaluate the background to many of the decisions in the war that they thought had been settled. The VENONA release in 1995 did not cause as great a stir as that earlier declassification, but it did lead many historians to re-evaluate the origins of the Cold War and the great American controversy of the 1940s and 1950s about disloyalty in the United States government. The VENONA decrypts do answer many questions about that earlier era and its controversies, although, of course, the decrypts cannot answer all questions or settle all issues – and may even raise a few new questions of their own.

But, if nothing else, the VENONA decrypts do show that at the beginning of the Cold War, there really were some reds under some beds.

David Hatch, PhD, American University, has held a variety of analytic and staff positions at NSA since 1973. He joined NSA's Center for Cryptologic History in 1990 becoming the NSA Historian in 1993. Dr. Hatch is the author of many histories of cryptology and NSA and has occasionally contributed to television documentaries.