Introductory History of VENONA and Guide to the Translations

Introductory History of VENONA and Guide to the Translations

THE VENONA PROJECT

On 1 February 1943, the U.S. Army's Signal Intelligence Service, a forerunner of the National Security Agency, began a small, very secret program, later codenamed VENONA. The object of the VENONA program was to examine, and possibly exploit, encrypted Soviet diplomatic communications. These messages had been accumulated by the Signal Intelligence Service (later renamed the U.S. Army Signal Security Agency and commonly called "Arlington Hall" after the Virginia location of its headquarters) since 1939 but had not been studied previously. Miss Gene Grabeel, a young Signal Intelligence Service employee who had been a school teacher only weeks earlier, started the project.

Arlington Hall before the war
(This postcard was used by army recruiters.)

The accumulated message traffic comprised an unsorted collection of thousands of Soviet diplomatic telegrams that had been sent from Moscow to certain of its diplomatic missions and from those missions to Moscow. During the first months of the project, Arlington Hall analysts sorted the traffic by diplomatic mission and by cryptographic system or subscriber.

Initial analysis indicated that five cryptographic systems, later determined to be employed by different subscribers, were in use between Moscow and a number of Soviet overseas missions. It also became apparent that one system involved trade matters, especially Lend-Lease. The other four systems appeared to involve the Soviet Foreign Ministry in Moscow in communication with its missions abroad.

Further analysis showed that each one of the five systems was used exclusively by one of the following subscribers (listed in descending order according to the volume of message traffic which had been collected):

1. trade representatives – Lend-Lease, AMTORG, and the Soviet Government Purchasing Commission;

2. diplomats – i.e., members of the diplomatic corps in the conduct of legitimate Soviet embassy and consular business;

3. KGB – the Soviet espionage agency, headquarters in Moscow and Residencies (stations) abroad;

4. GRU – the Soviet Army General Staff Intelligence Directorate and attachés abroad;

5. GRU-Naval – Soviet Naval Intelligence Staff.

THE VENONA BREAKTHROUGHS

From the very beginning in February 1943, the analysis of the traffic proved slow and difficult. Then in October 1943, Lieutenant Richard Hallock, a Signal Corps reserve officer who had been a peacetime archaeologist at the University of Chicago, discovered weaknesses in the cryptographic system of the Soviet trade traffic.

2

This discovery provided a tool for further analytic progress on the other four cryptographic systems.

During 1944, the skills of other expert cryptanalysts were brought to bear on this Soviet message traffic to see if any of the encryption systems of the messages could be broken. One of these cryptanalysts, Cecil Phillips, made observations which led to a fundamental break into the cipher system used by the KGB, although he did not know at the time who used the system. The messages were double-encrypted and of enormous difficulty. In spite of Arlington Hall's extraordinary cryptanalytic breakthroughs, it was to take almost two more years before parts of any of these KGB messages could be read or even be recognized as KGB rather than standard diplomatic communications.

Three closely spaced counterintelligence events occurred in 1945 that VENONA decrypts were able to amplify. First, the FBI carefully questioned Whittaker Chambers, whose earlier efforts to disclose details about Soviet espionage in the U.S. in the 1930s had gone unheeded. Second, Igor Gouzenko, a GRU code clerk, defected in Ottawa. Third, in late 1945 Elizabeth Bentley, a veteran KGB courier and auxiliary agent handler, went to the FBI and named names. While Gouzenko's revelations were important to Allied counterintelligence efforts, they had no bearing on the VENONA breakthroughs. Strong cryptographic systems like those in the VENONA family of systems do not fall easily. The VENONA decrypts were, however, to show the accuracy of Chambers' and Bentley's disclosures.

In the summer of 1946, Meredith Gardner, an Arlington Hall analyst, began to read portions of KGB messages that had been sent between the KGB Residency (station) in New York and Moscow Center. On 31 July 1946, he extracted a phrase from a KGB New York message that had been sent to Moscow on 10 August 1944. This message, on later analysis, proved to be a discussion of clandestine KGB activity in Latin America. On 13 December Gardner was able to read a KGB message that discussed the U.S.

presidential election campaign of 1944. A week later, on 20 December 1946, he broke into another KGB message that had been sent to Moscow Center two years earlier which contained a list of names of the leading scientists working on the Manhattan Project – the atomic bomb!


Meredith Gardner (left)

In late April or early May 1947, Gardner was able to read two KGB messages sent in December 1944 that showed that someone inside the War Department General Staff was providing highly classified information to the Soviets. These two messages are currently undergoing declassification review.

U.S. Army intelligence, G-2, became alarmed at the information that was coming out of Arlington Hall. An Arlington Hall report on 22 July 1947 showed that the Soviet message traffic contained dozens, probably hundreds, of covernames, many of KGB agents, including ANTENNA and LIBERAL (later identified as Julius Rosenberg). One message mentioned that LIBERAL's wife was named "Ethel."

General Carter W. Clarke, the assistant G-2, called the FBI liaison officer to G-2 and told him that the Army had begun to break

4

General Carter W. Clarke
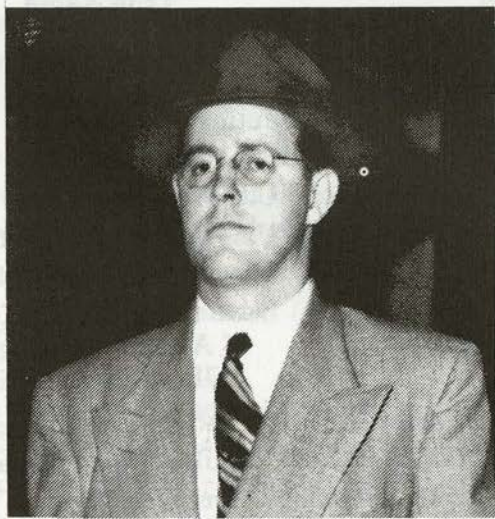
Robert Lamphere

into Soviet intelligence service traffic, and that the traffic indicated a massive Soviet espionage effort in the U.S.

In October 1948, FBI special agent Robert Lamphere joined the VENONA Project full time as the FBI's liaison and case controller for the VENONA espionage material. Also, by 1948 the British joined the VENONA effort; in particular, their signal intelligence service assigned full-time analysts to Arlington Hall. There was excellent cooperation between the two U.S. agencies and the U.K. over the many years of VENONA, in large measure a result of the early efforts of Robert Lamphere and Meredith Gardner.

A WORD ABOUT THE COVERNAMES

The VENONA messages are filled with hundreds of covernames (designations used in place of the real names to hide identities of Soviet intelligence officers and agents – i.e., spies or cooperating sources – as well as organizations, people, or places discussed in the encrypted messages). A number of public figures were also designated by covernames, while others in that category appear in the text of the messages by their true names. The following are examples of covernames recovered from the VENONA corpus:

Covername	True Name
KAPITAN	President Roosevelt
ANTENNA, later changed to LIBERAL	Julius Rosenberg
BABYLON	San Francisco
ARSENAL	U.S. War Department
THE BANK	U.S. Department of State
ENORMOZ	Manhattan Project/A-bomb
ANTON	Leonid Kvasnikov, KGB Chief of A-bomb espionage in KGB's New York City office

Arlington Hall and the FBI studied the covernames for leads to identities, grouping them into families of covernames. Some covernames came from mythology, some were Russian given names, and others were names of fish, etc. KAPITAN was easily identified

from the context as a good covername for President Roosevelt, but his covername was, nevertheless, outranked by those of persons of lower station, including KGB operatives covernamed PRINCE, DUKE, and GOD. Other KGB assets were just plain BOB, TOM, and JOHN, while Elizabeth Bentley had the covername GOOD GIRL. Very rarely, the KGB was careless in choosing a covername. For example, the covername FROST was used for KGB agent Boris Moros. The Russian word for "frost" is "Moroz."

THE VENONA TRANSLATIONS

There were about 2,200 VENONA messages translated. The VENONA translations now released to the public often show an unexpectedly recent date of translation because the breaking of strong cryptographic systems is an iterative process requiring trial and error and reapplication of new discoveries, leading to additional ones. Consequently, a message may have been reworked many times over the years as new discoveries enabled progress in the decryption and understanding of more and more of the text. Partial information was available from many messages as early as 1947 and later that year was provided to the FBI.

Almost all of the KGB messages between Moscow and New York and Moscow and Washington of 1944 and 1945 that could be broken at all were broken, to a greater or lesser degree, between 1947 and 1952.

There are still unreadable gaps in the translated messages. These are indicated as a number of code groups "unrecovered" or "unrecoverable." This means that the cryptanalysts were unable to break those portions of the messages.

SUCCESS RATE

The serial numbers of the VENONA messages indicate that the KGB and GRU sent thousands of messages between Moscow and the overseas recipients. Only a fraction of the total messages sent and received were available to the cryptanalysts. The messages which

have been exploited were never exploited in real time. In 1946 Meredith Gardner was working on KGB messages of 1944.

Arlington Hall's ability to read the VENONA messages was spotty, being a function of the underlying code, key changes, and the lack of volume. Of the message traffic from the KGB New York office to Moscow, 49 percent of the 1944 messages and 15 percent of the 1943 messages were readable, but this was true of only 1.8 percent of the 1942 messages. For the 1945 KGB Washington office to Moscow messages, only 1.5 percent were readable. About 50 percent of the 1943 GRU-Naval Washington to Moscow messages were read, but none from any other year.

VENONA MYTHS AND MISUNDERSTANDINGS

In spite of what has been written in a number of books and articles, Arlington Hall made the VENONA breakthroughs purely through sweat-of-the-brow analysis. There was no cryptanalytic assistance for Lieutenant Richard Hallock, Cecil Phillips, or Meredith Gardner and their colleagues from lost, discovered, or battlefield-recovered Soviet codebooks during the years in which the main analytic breakthroughs were made (through 1952). It was not until 1953 that a photocopy of a partially burned codebook (recovered by U.S. Military Intelligence in 1945) was discovered to be related to the VENONA cryptographic systems after another cryptanalytic breakthrough. The successful decryption of the VENONA messages was a triumph of analysis by a small group of intelligent and dedicated women and men working long hours in their cramped offices at Arlington Hall.

KGB OPERATIONS

Information in the VENONA materials reveals KGB tradecraft (i.e., the practical means and methods of espionage and counterespionage) of the time in great detail. Most VENONA messages concern operational/tradecraft matters. The sheer volume of data collected by KGB stations abroad was too great to be reported by telegram; instead the VENONA messages indicate that photocopies

8

of classified documents went to Moscow by courier. In one translation which is currently undergoing declassification review, KGB in New York informed Moscow that it had fifty-six rolls of film from their agent, covernamed ROBERT, and that this trove of classified material was to be sent off by courier to Moscow Center.

Information in VENONA translations describes the KGB's modus operandi in arranging meetings with their agents, with much attention given to the security of these secret meetings. Other messages describe KGB countermeasures against the FBI – countersurveillance, detection of bugging devices, and ensuring the loyalty of Soviet personnel in the United States. A particularly fascinating set of VENONA messages describes the KGB's efforts to locate Soviet sailors who had deserted from merchant ships in San Francisco and other U.S. ports. Some of the most interesting messages detail KGB assessment and recruitment of American Communists for espionage work.

KGB AND GRU SPIES AND ASSETS IN THE U.S.

Over 200 named or covernamed persons found in the VENONA translations, persons then present in the U.S., are claimed by the KGB and the GRU in their messages as their clandestine assets or contacts. Many of these persons have been identified, many have not been. These approximately 200 persons are separate from the many KGB and GRU officers who also appear in VENONA. One such asset, ROBERT, is found in VENONA translations several dozen times. Other covernamed persons were found only a few times. The majority of unidentified covernames in the New York KGB traffic appear three or fewer times.

THE AMERICAN COMMUNIST PARTY IN VENONA

Information derived from the VENONA translations shows the KGB's extensive contacts with the American Communist Party. Many of the espionage activities by members of the American Communist Party are reflected in the VENONA translations.

KGB ESPIONAGE AGAINST THE VENONA PROGRAM

A number of sources outside of signals intelligence reveal that the KGB learned early on that the U.S. had begun to study Soviet communications. In late 1945, KGB agent Elizabeth Bentley told the FBI that the KGB had acquired some limited information about the U.S. effort during 1944. Kim Philby, while assigned to Washington, D.C., 1949–1951, occasionally visited Arlington Hall for discussions about VENONA; furthermore, he regularly received copies of summaries of VENONA translations as part of his official duties. But if the Soviets knew something about what Arlington Hall was accomplishing, they could not, at any rate, get the messages back.

THE ROSENBERG/ATOMIC BOMB ESPIONAGE MESSAGES

VENONA translations that have been identified as associated with atomic bomb espionage messages are being released first. All but two of this group of forty-nine messages were KGB traffic; one is a GRU and one a Soviet diplomatic message.

These messages disclose some of the clandestine activities of Julius and Ethel Rosenberg, Harry Gold, Klaus Fuchs, David and Ruth Greenglass, and others such as the spy known by the covername MLAD or the equally important, but still unidentified, PERS. The role played by the person covernamed VEKSEL remains uncertain but troubling. A number of other covernames of persons associated with atomic bomb espionage remain unidentified to this day.

VENONA messages show that KGB officer Leonid Kvasnikov, covername ANTON, headed atomic bomb espionage in the U.S., but that he, like the Rosenbergs, who came under his control, had many other high-tech espionage targets such as the U.S. jet aircraft program, developments in radar and rockets, etc. As with most VENONA messages, the Rosenberg messages contain much information relating to KGB net control and tradecraft matters.

PERSPECTIVE

The VENONA program concerned KGB and GRU messages that were available to Arlington Hall codebreakers. Most of the messages which were collected were not successfully decrypted, and, short of a release of the KGB and GRU archives from the period, we may never know more about the KGB and GRU activities represented in the VENONA corpus of messages.

MORE TO COME IN 1995 AND 1996

Other VENONA translations covering many additional topics are currently undergoing declassification review.

Prepared by Robert Louis Benson
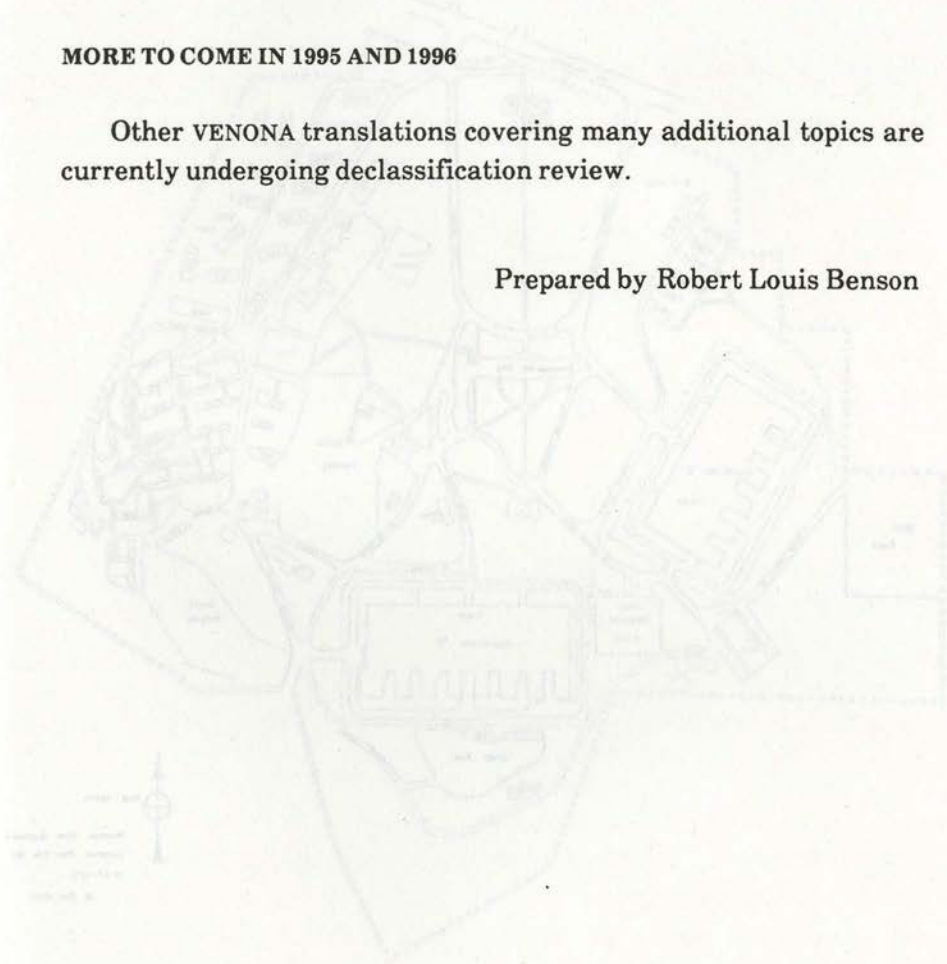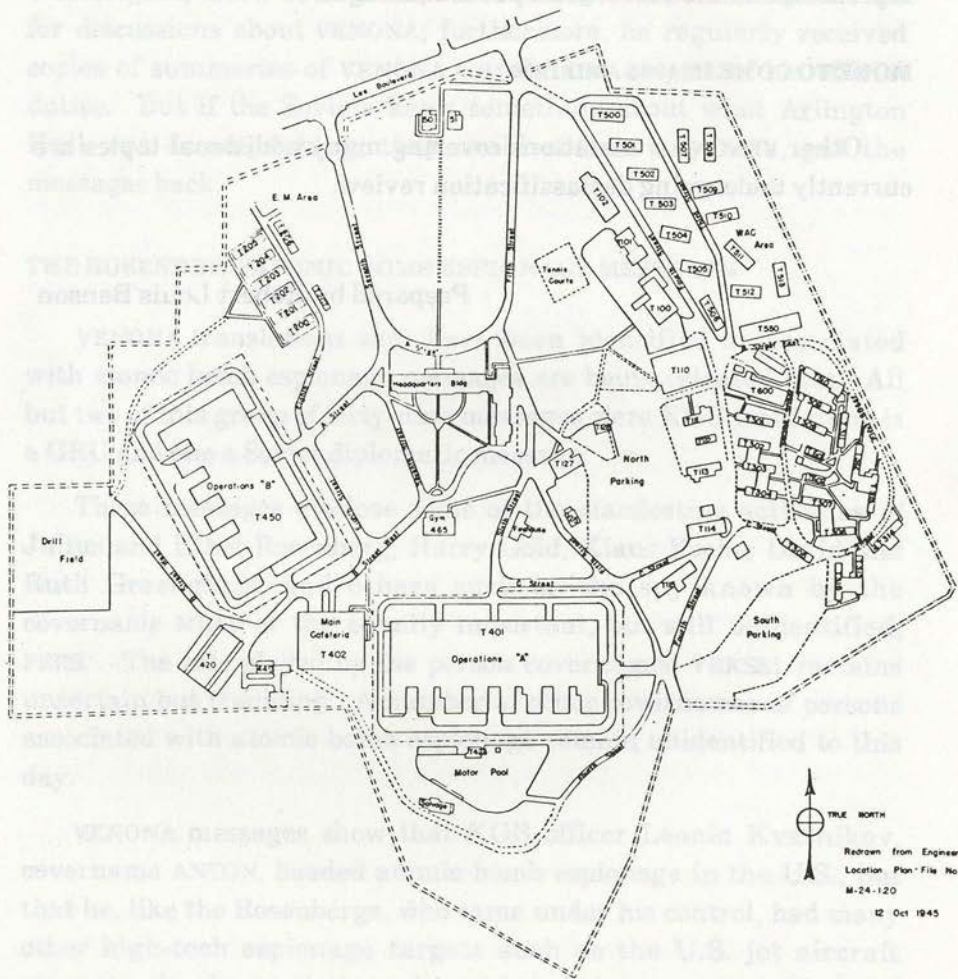
Map of Arlington Hall complex, circa 1940s.