DOCID: 4102958 UNCLASSIFIED

SECURITY CLASSIFICATION

Expedited AdW copy for D/DIR sig
10-4-95

NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER
D/DIR		

THRU	ACTION	EXREG SUSPENSE
Exec/DIR	☐ APPROVAL	
SUBJECT	☒ SIGNATURE	KCC SUSPENSE
Note to DCI – VENONA 2 release	☐ INFORMATION	ELEMENT SUSPENSE

DISTRIBUTION
ExReg, DDP, N5, N5P, N5P4

SUMMARY

As requested, this note and accompanying attachments are to inform the DCI of the 12 October date for releasing the second set of declassified VENONA documents to the public.

COORDINATION / APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
N5					
N5P	J. Cavanaugh (has seen 10/4)	3083			

ORIGINATOR	ORG	PHONE (Secure)	DATE PREPARED
Judith A. Emmel, Chief Judith A. Emmel	N5P4	963–5825	4 October

FORM A6796 FEB 94
NSN: 7540–FM–001–5465
COMPUTER FACSIMILE

Classified by:

Declassified on:

Approved for Release by NSA on 07-03-2014, FOIA Case # 42771

SECURITY CLASSIFICATION

UNCLASSIFIED

Deputy Director

04 October 1995

Dear Mr. Deutch:

Preparations are almost complete for the VENONA II release on 12 October. This release comprises over 250 KGB–GRU messages between the New York Residency and Moscow Center during 1942 to 1943.

Attached is the press release we will provide to interested media on 10 October. Also included is the second VENONA history and copies of the declassified documents, with several items of interest tabbed. My Public Affairs staff will meet with your OPA this week to finalize the details of this second release.

On 12 October the documents will be made available to the public and media. To do this expeditiously, we are using the NSA Home Page on the Internet as a vehicle of dissemination. We believe this will help us reach a greater audience and will prove to be an excellent way to serve the public interest. In addition, our museum display will be updated on 12 October and Agency historians will be on–hand that day to answer any visitor's questions about the VENONA project.

We are close to our planned release schedule. Considerable energy went into solving a number of privacy issues before the release; those issues have been addressed. We plan on making the third release, which will be about 600 messages, sometime in early 1996, probably January.

Sincerely,

Bill

William P. Crowell

Encls:
a/s

Honorable John M. Deutch
Director of Central Intelligence
Room 7D6011
Langley, VA

DOCID: 4129952

(b)(5)

VENONA Historical Monograph # 2:

The 1942-43 New York-Moscow KGB Messages

For further information or additional copies, contact the Center for Cryptologic History, National Security Agency, Fort George G. Meade, Maryland, 20755-6000, ATTN: E322.

The release of VENONA translations involved careful consideration of the privacy interests of individuals mentioned, referenced, or identified in the translations. Some names have not been released when to do so would constitute an invasion of privacy.

INTRODUCTION

The U.S. Army's Signal Intelligence Service, usually called "Arlington Hall" after the location of its headquarters, began a program to examine what it believed to be Soviet diplomatic and trade communications on 1 February 1943. Arlington Hall had on hand an unsorted collection of encrypted Soviet telegrams that had been collected intermittently since 1939. Starting with this corpus, while continuing to collect additional message traffic, Arlington Hall commenced its attacks against the Soviet diplomatic cryptographic systems used in the traffic. The project to analyze and translate these messages, which turned out to include Soviet KGB and GRU spy messages in addition to diplomatic and trade messages, eventually was named "VENONA." The story of this effort was outlined in *Introductory History of VENONA and Guide to the Translations*.

The first public release of translated VENONA materials, signals intelligence which had provided an insight into the alarming and hitherto unappreciated breadth and depth of Soviet espionage activities within the U.S., was in July 1995. That release was a compilation of forty-nine VENONA translations which related to Soviet espionage efforts against U.S. atomic bomb research, including messages about the Rosenbergs and the Manhattan Project.

This second release, and subsequent releases of the remaining approximately 1,800 VENONA translations, will not be thematic but, rather will be arranged chronologically by communications link. This monograph provides an overview of the content of the messages

between the New York KGB Residency and Moscow Center from 1942 to 1943, which are the object of this second release.

MESSAGES FROM THE KGB NY RESIDENCY TO MOSCOW CENTER

Although KGB and GRU communications between New York and Moscow during 1939–1941 were in a cryptographic system that could not be broken, a comparison of the New York-Moscow KGB and GRU message counts between 1939 and 1941 indicates that, at least in the U.S., the GRU may have been the more active Soviet intelligence agency up until that time. For example, in 1940 the NY GRU sent an estimated 992 messages to Moscow while the KGB sent only an estimated 335 messages. Furthermore, later releases of the VENONA translations of 1944 and 1945 messages will show that a number of KGB espionage personalities had previously been GRU assets (or possibly COMINTERN agents under GRU control). In 1942 there were nearly 1,300 KGB New York-Moscow messages, but only twenty-three were successfully decrypted and translated. In 1943, however, there were a little over 1,300 messages with over 200 decrypted and translated.

THE COMINTERN AND THE SOVIET INTELLIGENCE SERVICES

The COMINTERN (Communist International) was a Soviet-controlled organization that conducted liaison with the national Communist parties of various countries, including the United States, in order to further the cause of revolution. Moscow issued guidance, support, and orders to the parties through the apparatus of the COMINTERN. Nevertheless, Stalin publicly disbanded the COMINTERN in 1943. A Moscow KGB message to all stations on 12 September 1943, message number 142, relating to this event and included in this release, is one of the most interesting and historically important messages in the entire corpus of VENONA translations. This message clearly discloses the KGB's connection to the COMINTERN and to the national Communist parties. The message details instructions for handling intelligence sources

within the Communist Party after the disestablishment of the COMINTERN. The translation being released is of the Moscow-Canberra message, which was the only message of those sent to all the Residencies that was successfully decrypted.

KGB ORGANIZATION IN THE UNITED STATES

During the VENONA period, the KGB had U.S. Residencies (offices) in New York, Washington, and San Francisco – the latter residency was not established (or possibly reestablished) until December 1941. There also was a geographic Sub-Residency in Los Angeles.

The VENONA translations showed that the KGB New York Residency operated under three official institutional cover arrangements – the Soviet consulate, the trade mission (AMTORG/Soviet Government Purchasing Commission), and TASS, the Soviet news agency. Other KGB officers worked at various locations around the U.S. under Purchasing Commission cover, often as factory inspectors working on Lend-Lease matters.

During 1942–43, General Vassili M. Zubilin (true name: Zarubin) was the KGB Resident (chief) in New York. In 1943 he was transferred to Washington to become Resident there. Zubilin, known in VENONA by the covername MAXIM, signed many KGB telegrams. His wife, Elizabeth, was a KGB colonel who had the covername VARDO. There are indications that Zubilin/MAXIM was the senior KGB officer in the U.S. For example, the KGB Residency in Washington did not send messages until late 1943 after Zubilin arrived there. Before that, the Washington espionage messages were sent by New York.

All KGB Residencies abroad came under the First Chief Directorate (Foreign Intelligence) of the Moscow Center. Lieutenant General Pavel Fitin, covername VIKTOR, ran the First Chief Directorate, and most VENONA messages from the Residencies are addressed to him.

General Vassili M. Zubilin

Elizabeth Zubilin

KGB officer Pavel Klarin, covername LUKA, succeeded Zubilin/MAXIM as Resident in New York. In 1944 Stepan Apresyan, covername MAJ, became the NY Resident. MAJ signed hundreds of VENONA messages. All these New York Residents worked under the cover of vice-consul.

Stepan Apresyan

Although most or all KGB officers in New York worked for the First Chief Directorate, their day-to-day operations were defined by what the KGB called a "Line." A Line worked against a specific target set or carried out some specialized function. A number of Lines are mentioned in the VENONA translations, and their

specialization can be either identified or easily inferred. Some, not all, of these may be seen in the 1942–43 messages:

Line	Target or Function
KhU Line	High-tech targets including the Manhattan Project, jet engines, rocket engines, radar (Julius Rosenberg's group worked under this Line)
White Line	Probably worked against the White Russians
Fifth Line	Security of the Soviet Merchant Fleet (probably connected to the Second Chief Directorate – internal counterintelligence – at Moscow Center)
Second Line	Watching nationalist or minority groups of interest to the Soviet state (e.g., the Ukrainians)
Technical Line "A"	Special work such as document forgery
Fellowcountryman Line	Liaison with the American Communist Party
Line of Cover	The institutional or personal cover of the KGB officer

Other organizations referenced in the VENONA materials include the Eighth Department at Moscow Center, which evaluated political intelligence; the special cipher office, which encrypted and decrypted the telegrams; the Center-KGB headquarters; and the "House" or "Big House," which probably meant the COMINTERN headquarters in Moscow (although it sometimes appears to be used interchangeably for Moscow Center).

Telegrams sent by the KGB Residency in New York were usually signed by the Resident (MAXIM, LUKA, or MAJ) and were addressed to VIKTOR, head of the First Chief Directorate. Sometimes telegrams were signed with the covername ANTON, head of the KhU Line, since Moscow Center gave him special authority to do so in 1944. In special circumstances, telegrams were addressed to or received from PETROV, believed to have been L.P. Beria, head of the Soviet security apparatus; however, PETROV might also have been

V.N. Merkulov, a principal deputy of Beria, who probably headed KGB operations from the latter part of 1943.

At least in the case of the New York Residency, we see what probably was the KGB in transition – trying to organize its espionage activities better while sorting out the impact of the dissolution of the COMINTERN. We also see considerable KGB interest in European and Latin American Communists, which presented opportunities for subversion, a classic COMINTERN methodology, rather than espionage. Nonetheless, the New York Residency had many espionage assets during this period and was aggressive, even reckless, and imaginative in trying to recruit or place people in sensitive positions.

The activities of a Soviet "Illegal" MER/ALBERT (covernames for KGB officer Iskak Akhmerov, who operated as a clothier) first come to light in the current release. VENONA provides some insight into Illegals used by Soviet intelligence, although with the exception of the noteworthy activities of Akhmerov and a GRU-Naval operation involving an Illegal, there are only a small number of other cases of Illegals mentioned in the VENONA translations. An Illegal was usually a Soviet citizen, a KGB or GRU officer, who operated under an alias with no visible connection to official Soviet establishments. Illegals had no diplomatic immunity, usually entering the country illegally – hence the term. More information on Akhmerov and the GRU-Naval case will appear in a later VENONA release.

THE TRANSLATIONS AND KGB CRYPTOGRAPHIC SYSTEMS

These VENONA translations of 1942–1943 messages occasionally are fragmentary and difficult to understand. The code itself was complex and difficult to exploit using pure analytic techniques. Moreover, the broad contextual sweep of the content of these messages vastly complicated the difficulty of reading these KGB systems.

The cryptographic systems used by the KGB's First Chief Directorate involved a codebook in which words and phrases were represented by numbers. These numbers were then further enciphered by the addition of random number groups, additive, taken from a so-called one-time pad. A one-time pad comprised pages of random numbers, copies of which were used by the sender and receiver of a message to add and remove an extra layer of encipherment. One-time pads used properly only once are unbreakable; however, the KGB's cryptographic material manufacturing center in the Soviet Union apparently reused some of the pages from one-time pads. This provided Arlington Hall with an opening. Very few of the 1942 KGB messages were able to be solved because there was very little duplication of one-time pad pages in those messages. The situation was more favorable in 1943, even more so in 1944, and the success rate improved accordingly.

In order to break into the system successfully, Arlington Hall analysts had first to identify and strip off the layer of additive in order to attack the underlying code. These two levels of encryption caused immense difficulty in exploiting the codebook, and many code groups were, therefore, never recovered. The KGB messages from 1942 through 1943 and into 1944 as well as from earlier years were based on one codebook version. The 1944–1945 messages were based on a new codebook.

RECOVERED CODEBOOKS

As noted in the first VENONA monograph, *Introductory History of VENONA and Guide to the Translations*, and as publicly stated at the time of the release of the first set of translations, the Arlington Hall breakthrough on the KGB cryptographic systems was accomplished entirely through sweat-of-the-brow analysis without the aid of any captured codebooks. Fundamental cryptanalytic breaks against the extra encipherment which overlay the various codebooks were made in 1943–1944 by Richard Hallock, Cecil Phillips, and a small team of experts, by their own cryptanalytic brilliance. The knowledge gained earlier about the extra encipherment layer allowed Meredith Gardner to break into the second KGB codebook in late 1946. The

majority of KGB messages between the U.S. and Moscow that have been solved employed this second KGB codebook and were broken between 1947–1952. These were based on a KGB codebook which Arlington Hall had never seen.

The KGB messages from 1942 and 1943 employed the earlier and more difficult codebook. These 1942–1943 messages, some of which are the subject of this current release, were not attacked successfully until 1953–1954, when a second major cryptanalytic breakthrough was made through pure analysis by Dr. Samuel P. Chew at NSA, the successor of Arlington Hall. It was only after this second major breakthrough that a partially burned KGB codebook, which had been found in 1945, was able to be identified as the codebook employed in this system and to be put to use in attacking these messages.

A Military Intelligence team headed by Lieutenant Colonel Paul Neff, acting under Arlington Hall direction, had obtained a photocopy of this partially burned codebook at a Nazi Foreign Office signal intelligence archive located in a castle in Saxony during the last days of World War II in Europe. Neff's team got the material back to U.S. lines only the day before Soviet occupation forces moved into the area. The Nazis had acquired this codebook, and others, from the Finns, who had taken them from the Soviet consulate in Petsamo, Finland, on 22 June 1941. KGB officers in the consulate

Paul Neff **Oliver Kirby**

had succeeded only in partially burning the codebook before the facility was overrun. At about the same time, Lieutenant Oliver Kirby, also connected to Arlington Hall, recovered related cryptographic material while on a special mission in Schleswig, Germany. (Both Neff and Kirby later became senior civilian officials at Arlington Hall and later with NSA.)

KGB System	Message Translations by Arlington Hall	Help from Captured Codebook?
pre-1939 into 44	1953–54 & later	Some after initial analytic breakthrough
1944–45	late 1946–52 & later	None

NEW YORK KGB TRADECRAFT AND OPERATIONS, 1942–1943

Several KGB tradecraft terms that appear frequently in the VENONA translations are defined below:

PROBATIONERS: KGB agents

FELLOWCOUNTRYMAN: member of the American Communist Party

WORKERS or CADRE: KGB officers

PUT ON ICE or IN COLD STORAGE: deactivate an agent

LEGEND (A): cover story

NEIGHBORS: how the KGB referred to GRU and vice versa

The following references identify VENONA translations that give examples of KGB tradecraft and operations:

- KGB agents in the OSS: No. 880, 8 June 1943; No. 782, 26 May 1943
- NY KGB recruiting proposals: No. 854, 16 June 1942; No. 424, 1 July 1942; Nos. 1132–33, 13 July 1943
- An unidentified KGB agent in the company of President Roosevelt and Prime Minister Churchill (note that the Illegal

MER, later known as ALBERT, signed the message): No. 812, 29 May 1943

FUTURE RELEASES OF TRANSLATIONS DURING 1995–96

- KGB New York and Washington, DC, 1944–45 messages
- KGB San Francisco and Mexico City, 1942–46 messages
- GRU New York and Washington: GRU-Naval Washington: 1943 messages
- KGB and GRU non-U.S., non-Mexico (e.g., Montevideo): 1940–1946 messages

The 1944–1945 New York and Washington message release will be very large (over 500 translations) and should be of considerable historical interest.

By Robert Louis Benson