THE LINK

4th Edition May 2012

NATIONAL CRYPTOLOGIC MUSEUM FOUNDATION

AN INQUISITIVE MIND: JOHN NASH LETTERS

The National Cryptologic Museum's newest exhibit, "An Inquisitive Mind: John Nash Letters," features copies of correspondence between Dr. John Nash and the National Security Agency (NSA).

In 1955, while at the height of his career, Dr. Nash wrote a series of letters to NSA, outlining his ideas on an encryption-decryption machine. The agency acknowledged receipt of the letters but never adopted his proposals. Ultimately the letters were preserved with NSA's analysis in a collection of unsolicited correspondence. Nash is best known for his game-theory research as a graduate student at Princeton University. His work would earn him the Nobel Memorial Prize in Economic Sciences in 1994, and in 2001 his life would be profiled in the movie A Beautiful Mind.

The unclassified letters and the agency's analysis, portions of which were classified, remained protected in NSA's records center until 2011, when the entire collection was reviewed and declassified. The entire collection is being formally accessioned to the National Archives and Records Administration and will be available for public viewing later this year.

Renowned mathematician Dr. John Nash wrote a series of letters to NSA in the 1950s proposing a new encryption-decryption machine. Copies of his letters are on display at the National Cryptologic Museum. (NSA Photo)

Copies of Nash's letters are on display at the National Cryptologic Museum (NCM) with complete copies available for review in the museum's library and on the museum's web page at http://www.nsa.gov/public_info/_files/nash_letters/nash_letters1.pdf. The Nash letters were also recently featured on the National Geographic Channel's (NGC) program, "Inside the NSA". For more information on the program, please visit the NGC web site: http://channel.nationalgeographic.com/channel/.

The Nash letters are but one of the exciting new exhibits on the horizon at the NCM. Currently the staff is working on new displays honoring the NSA's 60th Anniversary and cryptology during the American Revolution. Finally, as was noted last month, the NCM is still looking for former Agency employees to serve in a volunteer capacity as docents. Please contact the museum curator at 301-688-5849 if you are interested.

Patrick Weadon, Curator
National Cryptologic Museum

In this issue of THE LINK

SIGINT SUPPORT TO COUNTERINTELLIGENCE:
THE NATIONAL CRYPTOLOGICAL MUSEUM LIBRARY COLLECTION

The National Cryptologic Museum (NCM) library contains remarkable collections of decrypted Soviet intelligence service radio messages of the 1930's and 1940's. In order of their exploitation there are three sets of Soviet messages, codenamed by the U.S. and UK as MASK, ISCOT and VENONA.

The NCM is the only place in the U.S. holding complete sets of this material. All three groups of published product show unambiguously the huge Soviet clandestine networks, all dependent on the various national communist parties -- and this includes the American Communist Party -- that were completely under Moscow's control.

This article will review briefly each set of materials. As the author was largely responsible for the release of all three, there will be some discussion of the declassification process.

Since most readers are familiar with VENONA, the emphasis in that section is on KGB agent Bill Weisband and the Soviet communications/cryptologic change of 1948, which was a tremendously important and unfortunate event for allied Sigint. Hall of Honor member Cecil Phillips assisted the author in much of the research on these three collections, as will be noted.

MASK

MASK was the British codeword for the UK collection and decryption of clandestine Communist International (COMINTERN) radio messages sent to and from outstations and Moscow from 1930-37. These messages were decrypted at the British Government Code and Cipher School (GCCS, a predecessor to today's GCHQ) by Colonel John Tiltman.

There are about 14,000 MASK messages, 1934-1937, held in the NCM library. The l930-33 messages cannot be found in GCHQ or NSA archives.

As the U.S. and UK withheld from each other their Russian Sigint programs until the end of World War II, MASK first became available to Arlington Hall in l945-46 during Cecil Phillips' liaison visits to GCCS where he was given a full set of MASK. The later odyssey of MASK is complicated and unclear, for example it is not certain when and how MASK reached the FBI, Military Intelligence (G-2) and CIA.

In the later 1990's, following the completion of the VENONA releases, I asked GCHQ to declassify MASK and send me copies of all available messages. GCHQ promptly agreed.

MASK messages to and from Moscow involved radio stations in the U.S. (on Long Island and Manhattan), the UK, Austria, China, Czechoslovakia, Denmark, France, Greece, the Netherlands, Spain, Sweden and Switzerland. Unfortunately for CI purposes, and history, there are only 100 plus U.S. MASK messages. Most U.S. messages were not collected.

The Mask messages are often brief and concern finances (Moscow funding of national communist parties), faked passports, secret travel arrangements, propaganda and dissemination of Moscow's line. True names were sometimes used in the encrypted messages, more often covernames or pseudonyms.

Following are extracts from several U.S. MASK messages as examples of typical topics. All are Moscow to New York.

31 October 1935. "It seems to us that your campaign under slogan 'Keep Canada out of

war'… is not quite correct. Working class of each capitalist country can struggle against involving in war one's country [but] struggling against war in any part of the world… this strengthens our struggle in defense of U.S.S.R." (emphasis my own)

24 March 1936. "Urge you speed up departure of [American] students for radio school. Furthermore urge that party choose three comrades especially reliable and trusted, with good American passports for our chief work. Furthermore urge you choose five young comrades well tested and especially vouched for by party knowing well photography and with good American passports."

30 March 1936. "In addition of previous communications, please inform us:

1. What short course for radio operators are there in your country [U.S.]
2. Are there private courses, under whose control are they, are people who finish these courses registered somewhere…?"

29 April 1936. "Confirm receipt of new address for couriers:

Dr. Victor Hansard, dentist, 31 Union Square, New York City"

12 June 1936. "Earl [Browder] must cable answer regarding 15 United States veterans [military veterans] invited to Russia for tour and month at [resort]…"

Browder, head of the American Communist Party, and Harry Pollitt, the head of the British Communist Party, are in many messages, as are later luminaries such as Jomo Kenyatta.

The MASK messages went off the air in 1937, date of resumption unknown. This probably had to do with the purge of COMINTERN headquarters in Moscow where most of these true believers were shot or sent to the Gulag.

While MASK gave the British extraordinary insight into UK communist party treachery, the overall international value of MASK messages probably exceeded the CI analytic capability of then tiny MI-5.

ISCOT

In early 1943, at a meeting between the chief of the Secret Service ("C"), MI-6, and the Director General of the Security Service (MI-5), it was decided that the UK should resume work on Russian communications systems (this work having been suspended soon after 22 June 1941). During 1942 the British Radio Security Service (RSS), an intercept arm of MI-6 and GCCS, had discovered extensive Russian illicit radio links, apparently KGB, GRU and COMINTERN. It was decided to concentrate on COMINTERN.

A GCCS group headed by Professor Bernard Scott (thus the codename ISCOT) ran this effort from 1943-1945. Some 1484 messages were decrypted and translated. ISCOT messages were mainly between outstations in German-occupied Europe and Moscow, especially Yugoslavia and Italy. These translations gave the UK a window into affairs behind German lines and Soviet plans for post-war Europe.

As with MASK, the British gave Cecil Phillips a set of these translations in 1945-46 and again there is uncertainty about further dissemination to FBI and CIA. After success in declassification of MASK, I asked GCHQ to declassify and give me copies of ISCOT. This was done quickly.

Cecil Phillips concluded from the crypto systems – and he and I concluded from the text of the messages – that they were probably a mixture of COMINTERN, Partisan and GRU communications.

The material is of great historical interest especially as many messages were broken and disseminated close to time of transmission, or at least while still relevant. Following are extracts or summaries of several representative ISCOT messages.

30 April 1943, a message relayed via uncertain links: "From France. We have received a communication from our Polish friends and they tell us [of an] attack on a concentration camp during which hundreds of comrades were freed."

3 November 1943, from Moscow to (?): "Kitty who passed through your post to Berlin has been arrested in Kutno. Please take necessary steps that all people who have been in contact with her change their addresses immediately."

25 February 1944, Yugoslavia to Moscow: A long message discussing events in Dalmatia, Bosnia, Herzegovina, and Slovenia, including a report that Himmler had met with Chetnik leaders in Trieste.

9 February 1944, probably from Italy to Moscow: This message describes Soviet soldiers fighting for the Germans, for example the Turkestan division, also a German led Ukrainian battalion "composed of 600 men all former Red Army men." The message reports that: "The Germans first mobilized the men of Turkestan, the Khirghizi and Eastern Asiatics, when there were no more of them left they began to mobilize Russians proper."

31 May 1944, Yugoslavia to Moscow: This message discusses how the Slovenes welcome a new Yugoslavia under Marshal Tito.

2 February 1944 to Moscow: Various messages provide good military intelligence on German order of battle in Trieste and Fiume and bombing targets (with coordinates) for the BMW factory in Munich and nearby Dornier factory, as well as the Kraus locomotive factory near Aschlach.

3 April 1945: Moscow directs Italian communist partisans to occupy Turin, Milan and other important places before General Mark Clark's forces do. "Take all measures to realize this policy of ours."

Some ISCOT messages especially from Holland and Poland describe aspects of the Holocaust.

VENONA

VENONA was the final codeword for the 37 year effort (from 1943 to 1980) by NSA and its predecessors to decrypt and translate Soviet intelligence services' messages of the 1940's. GCHQ and the other British services and the FBI became involved in VENONA in 1947.

Copies of the 3000 VENONA message translations are held at the NCM library.

In 1990-1991 I began research on VENONA and eventually wrote a three volume history of the program. As VENONA, though inactive, was still compartment, the enthusiastic sponsorship of Steve Collier and Bill Crowell made it possible. Eventually this led to declassification and release of the "last and best" versions of all translations, an enterprise involving me, the DCI John Deutch, Senator Moynihan and Bill Crowell.

VENONA has now appeared in many books and articles and, from a historical standpoint, closes many cases, such as proving the guilt of the Rosenbergs and of Hiss and of others.

VENONA, and subsequent findings by historians Alan Weinstein, John Haynes and Harvey

Klehr, also clarifies the disastrous (for the U.S. and UK) communications/crypto changes of 1948. This is the matter of a VENONA covername ZVENO, Bill Weisband, a KGB agent at Arlington Hall.

During my first reading of the VENONA translations, it became apparent to me (and to Cecil Phillips) that hitherto unidentified covername ZVENO, appearing in three KGB messages, must have been Weisband. Nonetheless it took some years of research and investigation and revelations from the KGB archives to resolve the story which, however, is still incomplete.

The key is VENONA message KGB New York to Moscow, number 981, 23 June 1943. New York reports that ZVENO had recently completed a course in Italian at "…ington, Virginia." The unrecovered part of this message was obvious. ZVENO was to leave for London during July 1943. The KGB was to meet him at Leicester Square and password exchange is given in the message: the KGB man was to say, "Hello Bill, greetings from Grigorij." ZVENO was to reply, "[7 groups unrecovered] on the West Coast." The exchange was to be in English or Russian.

We later recognized a second ZVENO message as containing information that Lona Cohen and her husband Morris (later infamous KGB illegals in the UK) were connected to Weisband.

The third ZVENO message was in January 1945, from the KGB Center in Moscow to New York. KGB said that soviet naval intelligence was returning ZVENO to KGB control and that the re-activation meeting would be in New York City according to a described scenario.

Cecil and I, through research in records and interviews, tied all of the above to Weisband, making the equation ZVENO = William Wolf Weisband (if that really was his name) certain.

Weisband had supposedly been born in Alexandria, Egypt to Russian parents – although he was probably born in Odessa – and came to the U.S. in the late 1920s with his parents. He worked at various hotel and accounting jobs in New York City, moved to Los Angeles in 1941, joined the Army in 1942, and was commissioned a 2/Lt, Signal Corps in 1943. He passed thru Arlington Hall for a short refresher course in Italian (in which he was fluent) in 1943 and went to London in July 1943 for orientation and then to North Africa and Italy where he served as both a Sigint and COMSEC officer with the 849th SIS, the main Mediterranean theater cryptologic organization.

He returned to Arlington Hall probably in July of 1944 and by early 1945 was in the very secret Russian Sigint organization, then mostly working VENONA (at that time called JADE or BLUE).

In 1950 the FBI confronted Jones York, a West Coast aircraft engineer who had been identified through VENONA as covername IGLA. York said that he had been a KGB agent from 1934-44 and that his third (of four) KGB handlers was Bill Weisband.

Weisband, then a civilian employee with AFSA at Arlington Hall, was interviewed by the FBI. He denied espionage and was fired from AFSA. He later served a year in prison for contempt of a grand jury but was never charged with espionage.

Starting in 1946 the U.S. and UK had broken into all high grade Soviet ciphers and was making great progress in exploitation, almost as successful as with ULTRA during WWII. In 1948, all these Soviet systems disappeared and the U.S.-UK was left with almost nothing on the Soviet target. North Korea invaded South Korea in June 1950, without warning, in a war that was planned, partially directed, and partially fought by the Soviet Union. There was no advance warning from Sigint.

Continued on Page 7

(Facsimile of ISCOT message)

FILE.

TOP SECRET.

TO BE KEPT UNDER LOCK AND KEY: NEVER TO BE REMOVED FROM THE OFFICE.

No: ISCOT 1081.

Date: 19th March, 1945.

Service 16. Cypher 16 A.
To MOSCOW.

Call sign XES. Date: 27th May, 1945.
To: 01.
From: 05.
No: 67.

AMSTERDAM University. All professors gave notice collectively of their intention to resign. They were then warned that they had to withdraw this notice within 6 hours, otherwise they would all be shot by a firing squad. The professors then withdrew their notice.

D.D./S.P.(3).
Colonel Morton-Evans.

Continued from Page 5

Reviewing all the evidence, it now seems clear that the Sigint silence occurred because Bill Weisband had given the store away. He had been a KGB agent since 1934. He was probably in the Soviet Union in the early 30's at the Lenin School, the COMINTERN school. If we return to the MASK message we see that he was, in 1936, a student at the RCA radio school in New York City, as directed by the COMINTERN/ KGB.

In recent years the KGB has released some of their records, including ZVENO = Weisband. Those records include the KGB understanding, from 1948, that Weisband had told them that Arlington Hall had been reading all their messages – military, civil, atomic bomb. The Soviets fixed their problems because of Weisband.

Weisband's work resulted in what was probably the single greatest loss in intelligence in U.S. history. MASK and VENONA helped to piece the whole story together.

ACCESS TO NCM COLLECTIONS AND OTHER SOURCES

The NCM library's director, Rene Stein, has organized MASK, ISCOT, and VENONA in a helpful way and can assist those interested in access to the collections and to other sources of information on the collections.

Lou Benson, Editor

HISTORIAN'S CORNER

Even the Center for Cryptologic History (CCH) has urban legends. According to the story, when one of NSA's early historians paid a courtesy call on the Deputy Director, he said, "Hello, I'm Dr. Howe and I'm going to publish a history of AFSA."

Allegedly, the D/DIR responded, "Hello, I'm Dr. Tordella and no, you're not."

Whether this story is true or not, the Agency discouraged publishing history studies in NSA's earlier days.

When the CCH was established in 1989, the leadership envisioned a vigorous publications program. The feeling was then, as it is now, that while research and preservation of history are important, the CCH has failed if it does not communicate to others what it learns.

Because the Director had sponsored the CCH so that it would preserve our history and help the workforce to learn from it, publications were now encouraged.

CCH historians then and now adopted a style that seeks to avoid both "governmentese" and "academese." Our goal is to publish studies that are both valid from an academic standpoint and readable.

The first two CCH publications were a reprint of a classic, William Friedman's lectures on the history of cryptology, and a newly produced history, Thomas Burns' study of the establishment of NSA.

Since that time, the CCH has averaged several publications a year on a wide range of topics.

Over thirty-five CCH publications, many unclassified originally, some declassified, are available in softcopy on the NSA website, www.NSA.gov. From the website, you can also order hard copies, if you prefer to have a book you can hold or in which you can write marginalia. You can also request publications directly from the CCH by letter, phone (301-688-2338), or e-mail (history@NSA.gov).

David Hatch, NSA Historian

Join the National Cryptologic Museum Foundation

ANNUAL MEMBERSHIP APPLICATION

☐ Please begin/renew my membership in the Foundation

- ☐ Benefactor $10,000
- ☐ Patron $5,000
- ☐ Sponsor $1,000
- ☐ Donor $500
- ☐ Supporter $250
- ☐ Sustainer $100
- ☐ Individual $35

The Foundation is certified as a non-profit organization by the I.R.S.

Name: _____

Address: _____

City: _____

State: _____ Zip: _____

Phone: _____ E-Mail: _____

Date: _____

Please make your check payable to:
NCMF

The National Cryptologic Museum Foundation, Inc.

CONTACT US:
(301) 688-5436 & 5437
Fax (301) 688-5619
email: cryptmf@aol.com
http://www.cryptologicfoundation.org

MUSEUM TELEPHONE:
(301) 688-5849
Library (301) 688-2145

MUSEUM HOURS:
Monday - Friday - 9:00 a.m. - 4:00 p.m.
1st & 3rd Saturdays - 10:00 a.m. - 2:00 p.m.

The National Cryptologic Museum Foundation, Inc.
P. O. Box 1682
Ft. George G. Meade, Maryland 20755-9998

FORWARDING SERVICE REQUESTED

NONPROFIT
U.S. POSTAGE
PAID
FORT MEADE, MD
PERMIT NO. 43