DOCID: 4129927

TOP SECRET UI

SECURITY CLASSIFICATION

N5
Z
GC
LA BENSON

Per DDIR,
1. Response to DCI attached inside
2. Will have meeting with requisite folks to agree on groundrules for declassification and release.
DDIR done 5/15 PSM Re Deutch Reaction - M

NSA STAFF PROCESSING FO

Declassified and Approved for Release by NSA on 07-03-2014 pursuant to E.O. 13526, FOIA Case # 42771

TO
DIR

EXREG CONTRO

THRU
D/DIR, Exec Dir

SUBJECT
Response to DCI on VENONA - INFORMATION

MEMORANDUM [X]

DISTRIBUTION
DDP, OGC, N5, N5P, N5131 ,N5132, M5J, Z22, A952

SUMMARY

PURPOSE: To respond to DCI Deutch's query regarding VENONA ma

DISCUSSION:

--VENONA is the codename for the US/UK exploitation of encrypted KGB and GRU communications from 1937-48. Exploitation of these communications continued until as recently as September 1980 when a KGB message sent in 1943 was published.

--The issue of declassification/release of VENONA records is currently being considered attendant to Freedom of Information Act (FOIA) requests to NSA.

--The categories of VENONA material and our intended treatment of this information are as follow:

1. Translations - These can be released almost entirely once GCHQ agrees. The translations are at issue in two Freedom of Information Act (FOIA) requests. We intend to protect information which would continue to cause damage to the national security and information related to personal privacy. Information considered personal relates to individuals named in the translations whose association with or identification as suspected Soviet sympathizers/spies is not well known or is not widely available in the public domain. Enclosure 1 contains examples of translations which have been provided to GCHQ for illustrative purposes to aid in the British Government's determination. Information marked in yellow is that which we intend to protect, The portions highlighted in blue must be coordinated with other agencies, and those marked in green require further analysis. Also included on these examples are some explanatory notes regarding the protection of information and an indication of the FOIA exemptions which apply [e.g., (b)(1), (b)(3)].

2.Raw traffic/encoded intercepted messages and their decrypts. This material must be protected in its entirety to preserve intelligence sources and methods.

3. Supporting material (e.g., cryptanalytic worksheets, studies, technical reports, code books, non-NSA reports) - It is possible that some of this material may be declassified, but this material has not been studied closely because it is not at issue in the FOIA requests. A declassification decision on non-NSA reports would be made by the originating agencies.

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
DDP	5/12				
N5	for 18/5				
N5P	5/18/95				
M5J	Robert Benson 18 May 95	963-1978			
EXREG					

ORIGINATOR	ORG.	PHONE (Secure)	DATE PREPARED
Rona Lerner	N5131	963-5827	05/18/95

FORM A6796 FEB 94
NSN: 7540-FM-001-5465

Classified by: NSA/CSSM 123-2
Declassified on: OADR

SECURITY CLASSIFICATION

TOP SECRET UMBRA

4. Three-volume history written by Lou Benson and Cecil Phillips at Enclosure 2 and the backup material used to write the history - This material is not at issue in the FOIA requests and has not been closely reviewed. It is possible that portions could be segregated for release. A copy of this history will be provided to the CIA CI Center to replace the draft copy they are holding.

STATUS: We have been waiting for GCHQ's agreement to declassify portions of the translations. [redacted] NSA is prepared to begin a review of the translations to release to the FOIA requesters portions which no longer require protection. Because of the nature of the material, release would also be made to the National Archives and a press release would be issued.

(b) (1)

NOTE: TAB 1 material exemplifies data which may be released, after declassification (unmarked); data to be withheld (yellowed); other agency (general) data (green); and personal data (blued).

TAB 2 Is a copy of the recently published VENONA history with a 1-page executive summary.

JC.

DEPUTY DIRECTOR

19 May 1995

TO: DIRECTOR OF CENTRAL INTELLIGENCE

SUBJECT: Details of the VENONA Papers

Per your conversation with Admiral McConnell, attached is a summary of the VENONA project and a point paper on the status of declassifying and releasing the information.

This is an issue I have followed for most of my NSA career, perhaps longer than I would care to admit. I would certainly be happy to give you more information should you be interested. Also, we can provide you with the 3 volume history of VENONA, done by Lou Benson and Cecil Phillips, which was just printed last week.

It is our intent to declassify and release the details of this fascinating story as soon as we can get all the players to agree.

WILLIAM P. CROWELL

~~TOP SECRET UMBRA~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(5)

18 May 1995
INFORMATION

SUBJECT: Status of declassification and release of VENONA

DISCUSSION:

--Attached is a summary of the history of VENONA.

--The issue of declassification of VENONA records is currently being considered attendant to Freedom of Information Act (FOIA) requests to NSA.

--The categories of VENONA material and our intended treatment of this information are as follows:

1. Translations - These can be released almost entirely once GCHQ agrees. A 23 September 1994 NSA request to GCHQ sought British agreement that the entire VENONA collection no longer requires protection. The translations are at issue in two FOIA requests. We intend to protect information which would continue to cause damage to the national security and information related to personal privacy.

2. Raw traffic/encoded intercepted messages and their decrypts - We will protect in entirety to preserve intelligence sources and methods.

3. Supporting material (e.g., cryptanalytic worksheets, technical reports, code books, non-NSA reports) - Some of this material may be declassified, but it has not been studied closely.

4. Three-volume NSA history and the backup material used to write the history - This material is not at issue in the FOIA requests. We believe that Volume II could be released in large part, mainly translations and the analysis which provided leads to FBI. A copy of this history will be provided to the DCI CI Center to replace the draft copy it is holding.

NSA's POSITION: We have developed instructions for the declassification of the translations, and we are prepared to begin a review of the translations for release to the FOIA requesters and the National Archives. A press release would be issued to announce this. To process this material expeditiously, additional manpower will be required, with overall control to ensure that all that can be released is released and that only information which requires continued protection is withheld.

STATUS: NSA has been waiting for GCHQ's agreement to declassify portions of the translations.

ORIGINATOR: Rona Lerner, N5P, 963-5827

~~TOP SECRET UMBRA~~

Classified By NSA/CSSM 123-2
Declassify On: Originating Agency's Determination Required

18 May 1995
Lou Benson

VENONA - Summary History

Background Venona was the final NSA codeword covering our ability to decrypt a certain bloc of KGB, GRU and GRU-naval record traffic concerning Russian espionage: Russian messages sent, mostly between 1942-1946.

Period of Exploitation NSA predecessor (Army - Arlington Hall) started working Russian Dip 1 Feb 43; made first decrypt of KGB message traffic (imbedded in the Dip) in 1946. Series of special reports in 1947; flood of decrypts and translations starting in 1948. This same bloc of 1942-46 traffic was worked until 1 Oct 1980 when NSA shut down its Venona program. Worked in cooperation with GCHQ from 1948 on.

Statistics About 2200 translations published. Some 700 of these on NY < -- > Moscow lanes; other exploitable traffic on Mexico City, Wash DC, London, San Francisco, Stockholm, Canberra to/from Moscow lanes. Mostly KGB; modest amount of GRU. KGB NY outgoing messages for 1944 were 49% readable; also very good success rate for KGB Mexico City and San Francisco in 1944 and GRU-naval Washington 1943.

Cryptanalytic Technique A small Arlington Hall team discovered in 1944 that a depth of two existed in some of the traffic. It became apparent that KGB crypto production center had produced extra sets of some one time pads - if these could be identified and matched, decryption possible. Strictly an analytic process - US did not have any pads, codebooks etc until 1953, when we identified a KGB codebook in a collection of material grabbed from German Sigint center in 1945. By then, we had entered majority of exploitable messages.

What's in the Venona Translations The information that led to the arrest of the atomic bomb spy rings - Klaus Fuchs, the Rosenbergs, Harry Gold; info that broke up the Maclean-Burgess-Maclean group. Also proof of the espionage of Asst Secy of Treasury Harry Dexter White, Alger Hiss and 100+ others. Many covernames in the traffic remain unidentified though only a few look like major spies.

Problems Eleanor Roosevelt in the traffic - KGB planning to recruit or somehow use her; same for I.F. Stone. Arthur Goldberg (Supreme Court/ UN ambassador) in a important espionage message; Ed Levi (later Attorney General) may be in the traffic. Goldberg and Levi NOT Venona spies, but messages are a problem. Much of the material is very fragmentary which will raise many questions about what the missing words/phrases may be.

DOCID: 4129927

No Code

No Code

No Code

No Code

No Code

No Code

Code

No Code

Code

No Code

Code

No Code

No Code

18 May 1995
Lou Benson, M5

VENONA - Summary History

A set of the 3 volume history of Venona, just printed last week in final version is attached. Written by Lou Benson and Cecil Phillips.

Background Venona was the final NSA codeword covering our ability to decrypt a certain bloc of KGB, GRU and GRU-naval record traffic concerning Russian espionage: Russian messages sent, mostly between 1942-1946.

Period of Exploitation NSA predecessor (Army - Arlington Hall) started working Russian Dip 1 Feb 43; made first decrypt of KGB message traffic (imbedded in the Dip) in 1946. Series of special reports in 1947; flood of decrypts and translations starting in 1948. This same bloc of 1942-46 traffic was worked until 1 Oct 1980 when NSA shut down its Venona program. Worked in cooperation with GCHQ from 1948 on.

Statistics About 2200 translations published. Some 700 of these on NY < -- > Moscow lanes; other exploitable traffic on Mexico City, Wash DC, London, San Francisco, Stockholm, Canberra to/from Moscow lanes. Mostly KGB; modest amount of GRU. KGB NY outgoing messages for 1944 were 49% readable; also very good success rate for KGB Mexico City and San Francisco in 1944 and GRU-naval Washington 1943.

Cryptanalytic Technique A small Arlington Hall team discovered in 1944 that a depth of two existed in some of the traffic. It became apparent that KGB crypto production center had produced extra sets of some one time pads - if these could be identified and matched, decryption possible. Strictly an analytic process - US did not have any pads, codebooks etc until 1953, when we identified a KGB codebook in a collection of material grabbed from German Sigint center in 1945. By then, we had entered majority of exploitable messages.

What's in the Venona Translations The information that led to the arrest of the atomic bomb spy rings - Klaus Fuchs, the Rosenbergs, Harry Gold; info that broke up the Maclean-Burgess-Maclean group. Also proof of the espionage of Asst Secy of Treasury Harry Dexter White, Alger Hiss and 100+ others. Many covernames in the traffic remain unidentified though only a few look like major spies.

Problems Eleanor Roosevelt in the traffic - KGB planning to recruit or somehow use her; same for I.F. Stone. Arthur Goldberg (Supreme Court/ UN ambassador) in a important espionage message; Ed Levi (later Attorney General) may be in the traffic. Goldberg and Levi NOT Venona spies, but messages are a problem. Much of the material is very fragmentary which will raise many questions about what the missing words/phrases may be.