RSAConference2019
San Francisco | March 4–8 | Moscone Center


SESSION ID: BAC-T08

# Mechanical Backdoors in Cold War Encryption Machines

**Marcus H. Sachs**

Chief Security Officer
Pattern Computer, Inc.
@MarcusSachs

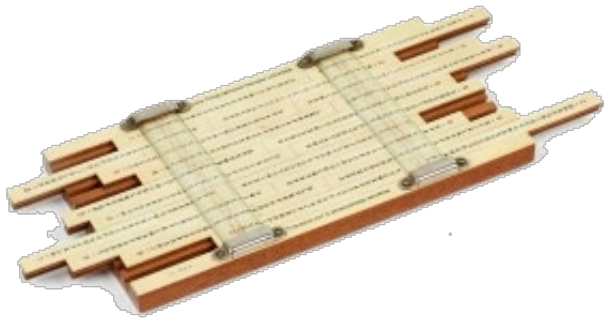
# Outline

- VERY Brief History Of Mechanical Encryption Machines
- Boris Hagelin And His Encryption Devices
- The William Friedman Papers
- A Gentlemen's Agreement
- What We Know About NSA's Initiative
- The Rest Of The Story

# VERY Brief History Of Mechanical Encryption Machines

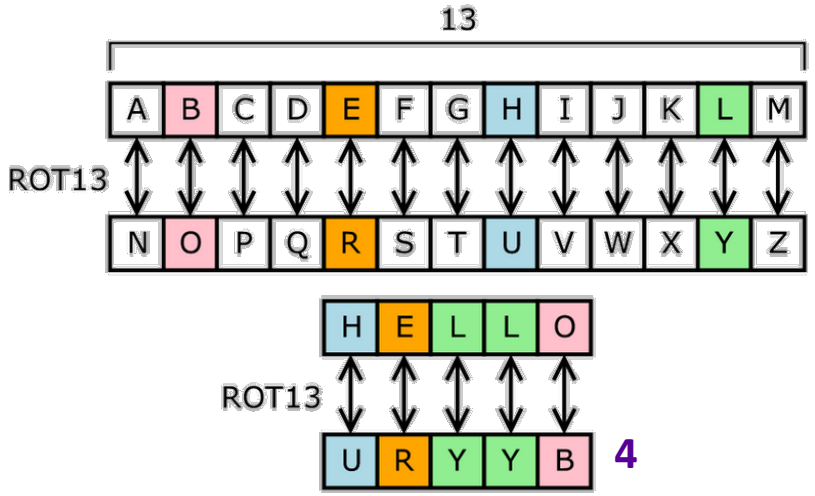
- First mechanical devices were leather strips wound around sticks

- Later devices used wood, ceramic, or metal



# How They Worked

- Most encryption algorithms work on two principles:
  - Substitution (each letter retains its position but changes its identity)
  - Transposition (each letter retains its identity but changes its position)
- Early mechanical devices typically used the *substitution* principle
  - Caesar cipher shifts each letter three places down the alphabet
  - ROT-13 shifts each letter 13 places, making it a symmetric cipher

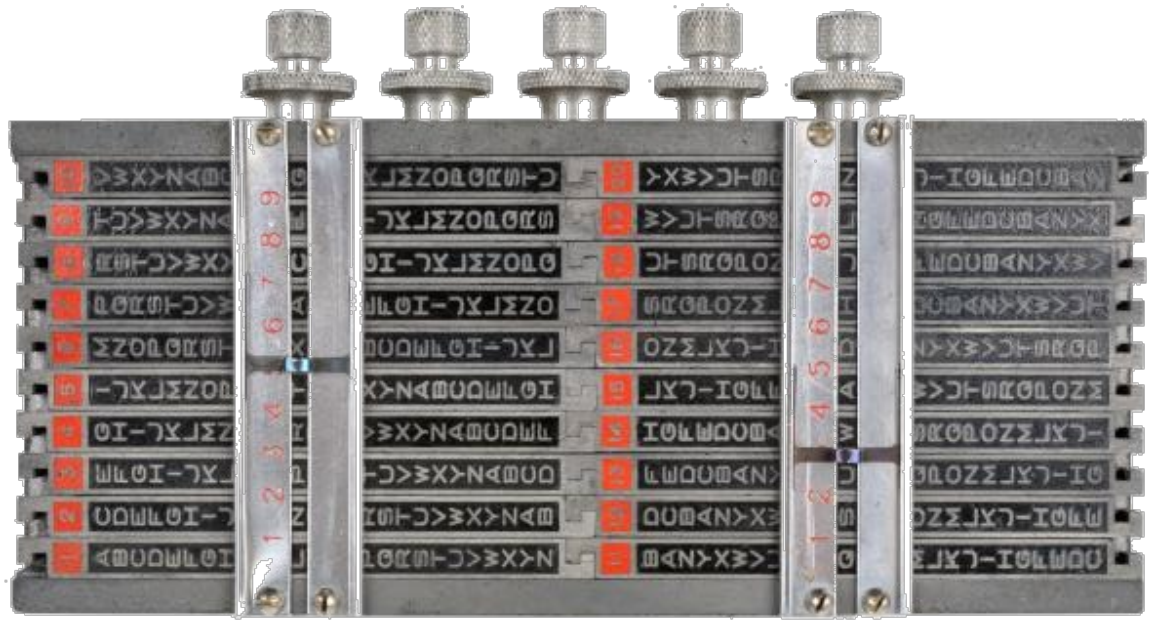


# Simple Mechanical Cipher Machines

- Until the invention of the radio in the very late 19th Century, speed and strength of encryption was not an issue
  - Messages took minutes or hours to deliver, even over a telegraph
  - Number of “eyes” that could intercept the message was limited
  - Code-breaking was a manual process, and could take days or weeks
- Battlefield encryption used substitution ciphers


# Businesses Needed Encryption, Too

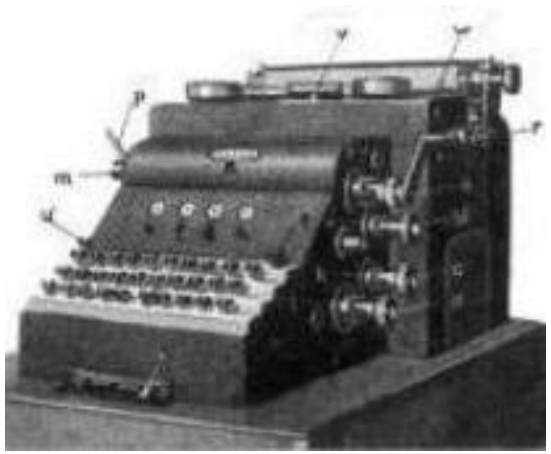
- Commercial messages via telegram were vulnerable to eavesdropping
- Code books and mechanical substitution devices were in common use by the turn of the century



# Rotor-based Cipher Machines

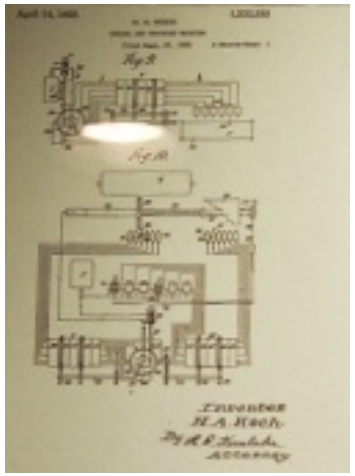
- Proliferation of radio in WWI created a need for faster encryption tools
- Typewriters and teletype machines were readily available in the 1910's and served as models for a new approach

Hebern, USA
1917



Scherbius, Germany
1918

Damm, Sweden
1919



Koch, Holland
1919

PATTERN COMPUTER

# The Infamous Enigma Machine

- Invented in 1918
- Major advance in ease of use and cryptographic strength
- Originally designed for commercial and business customers
- Adopted by German military in late 1920s and early 1930s
- Used into the 1960s

# Boris Hagelin And His Encryption Devices

- 1921 - first cipher machine developed while working for Arvid Gerhad Damm in Sweden
- 1935 – first mechanical machine under Hagelin's brand name of **A. B. Ingeniörsfirman Teknik** (later changed to **A. B. Cryptoteknik**)
- After WWII, company moved to Switzerland as **Crypto AG***
- Model numbers often reflect year of development
  - C-35 was developed in 1935
  - C-52 was developed in 1952


*__AG__ is the abbreviation of Aktiengesellschaft

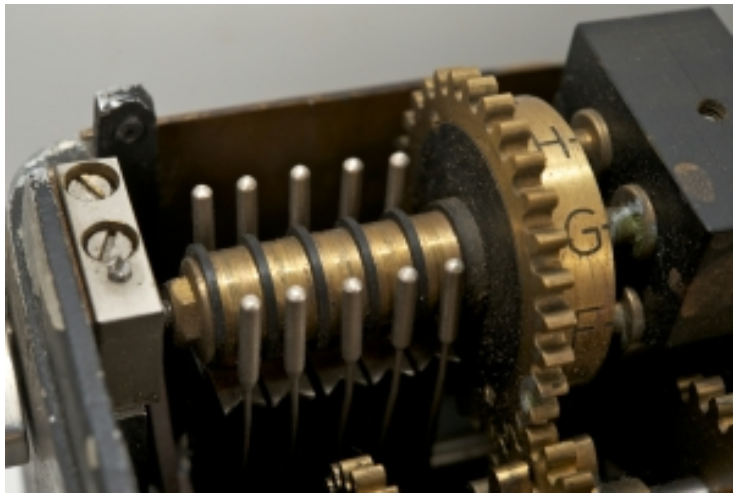
# Hagelin vs Enigma

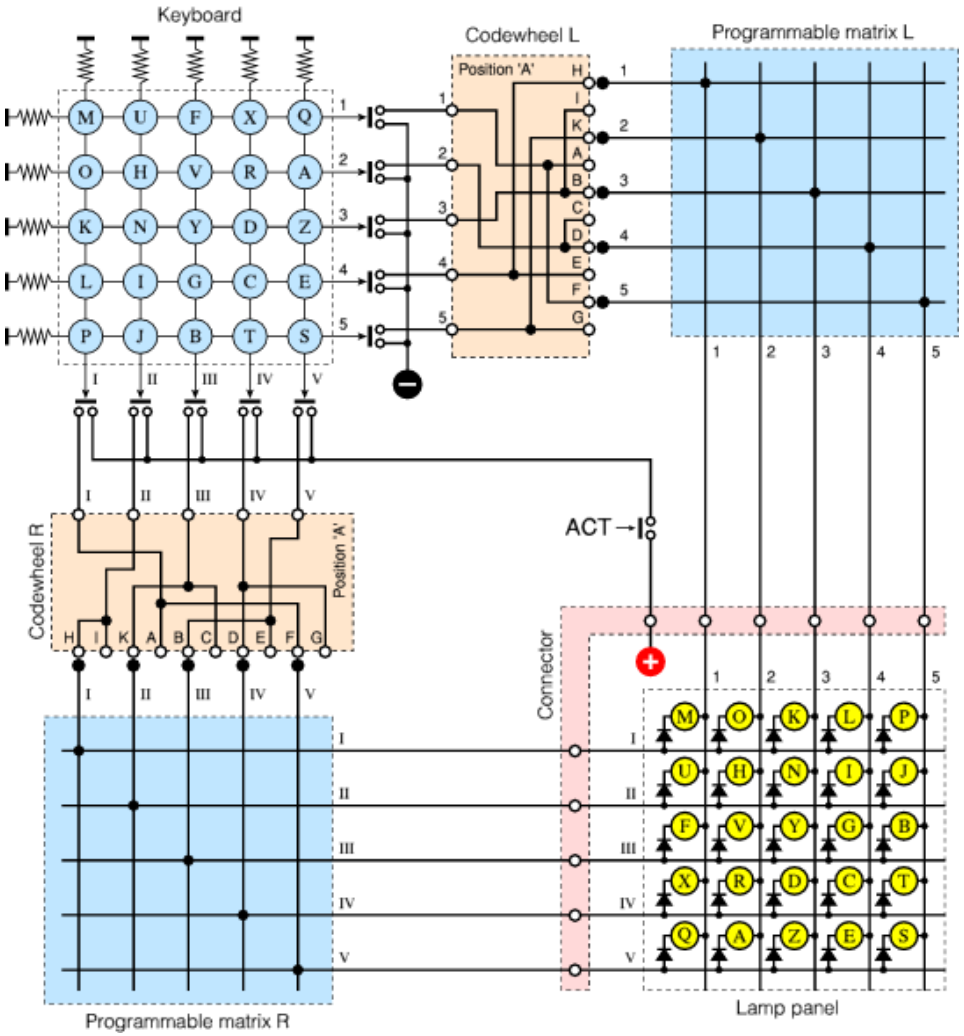
B-21 by Hagelin (1925)

Enigma by Heimsoeth und Rinke (1937)

# Inside the B-21

- Keyboard and lamp panel are similar to the Enigma
- Enigma used alphabet substitution; B-21 used coding wheels to scramble a 5x5 matrix





# Pin-and-Lug System versus Enigma-style Rotors-and-Bulbs

- Pin and Lug
  - Five or more wheels with pins, all relatively prime
  - 25-bar “drum” with lugs
  - Lugs interact with pins to create a pseudo-random stream of enciphered letters
  - No electric power – mechanical hand operation
- Rotors and Bulbs
  - Three or more rotors with 26 or more contacts
  - Rotation of rotors similar to a vehicle’s odometer
  - Pressing a key closes an electrical circuit
  - Battery or external power illuminates bulbs

http://www.nf6x.net/wp/wp-content/uploads/2009/02/M-209-B.wmv

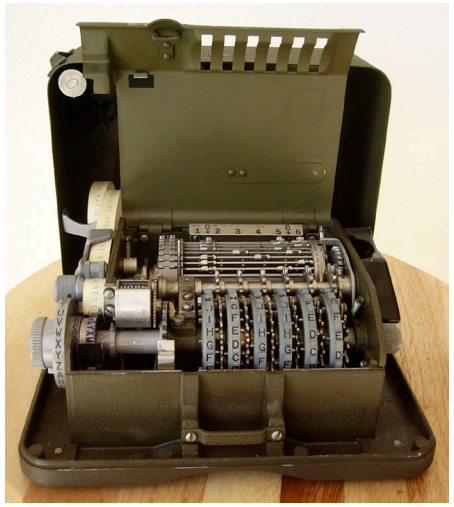
https://www.youtube.com/watch?v=mcX7iO_XCFA

# Various Hagelin Pin-And-Lug Devices


C-35

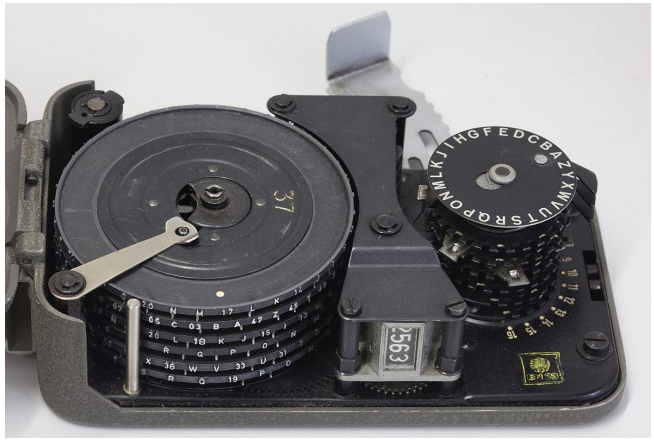
C-36

C-38



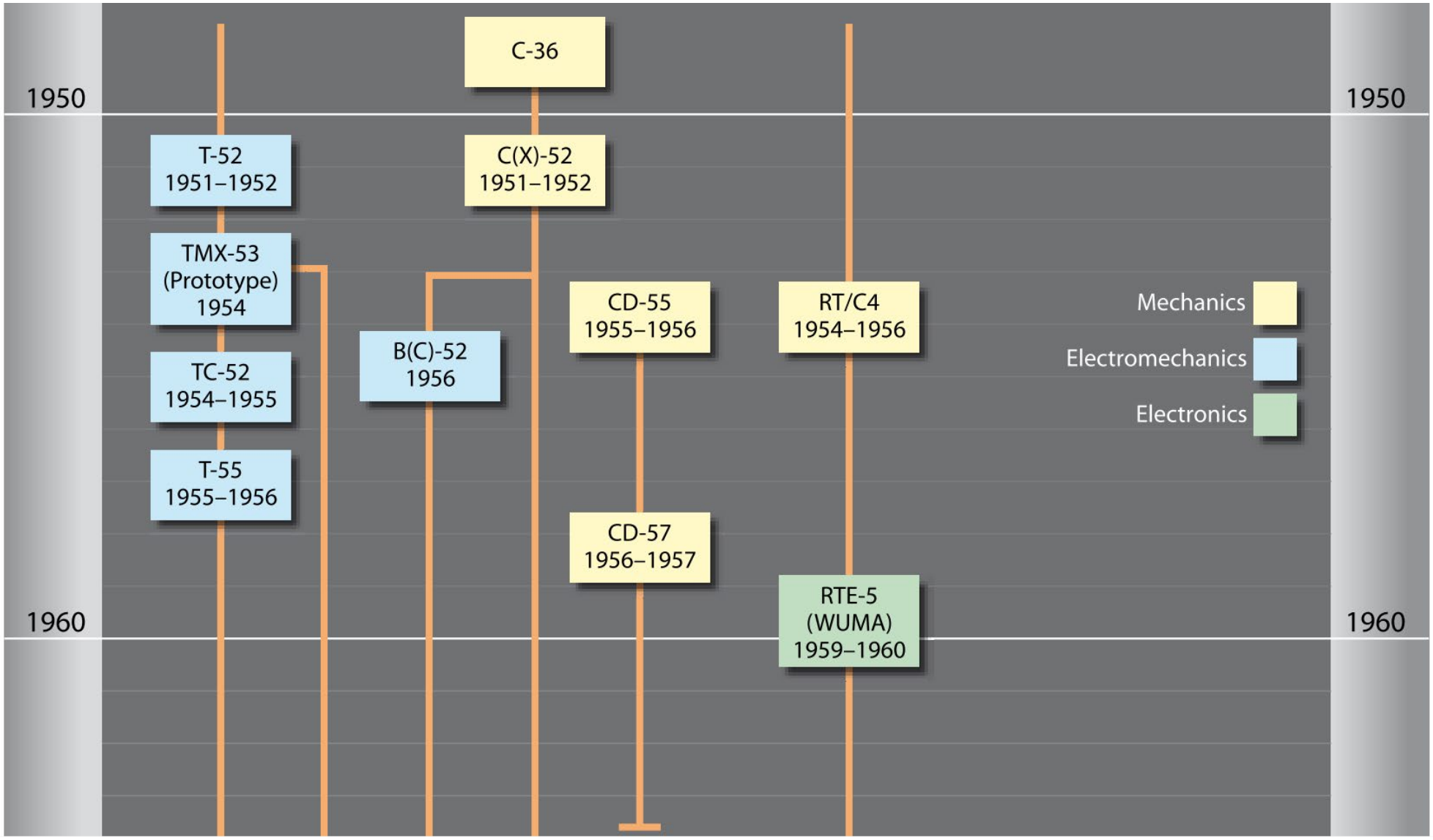
M-209

C-52 and CX-52



CD-57

# Crypto AG in the 1950s

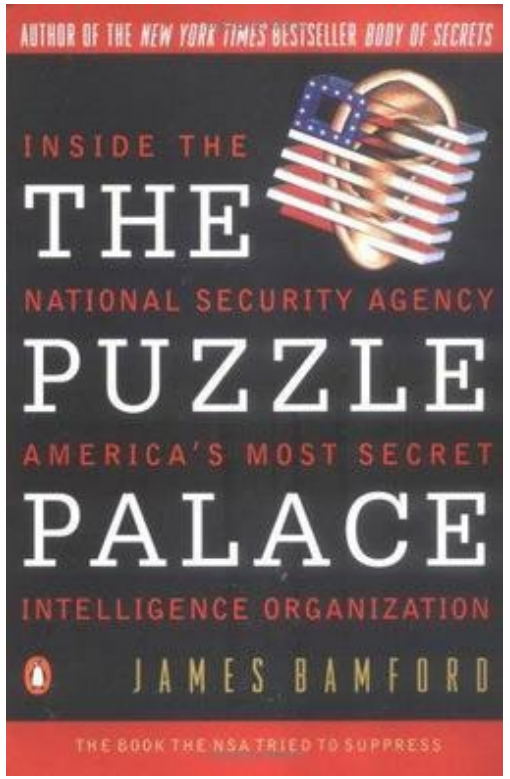


# William Friedman (September 24, 1891 – November 12, 1969)

- US Army cryptographer who ran the research division of the Army's Signal Intelligence Service (SIS) in the 1930s, and parts of its follow-on services at the National Security Agency (NSA) into the 1950s
- Married to Elizebeth Friedman, also a cryptographer
- Initiated a secret agreement with Crypto AG in 1954
- William and Elizebeth's personal papers were donated to the George C. Marshall Foundation in 1969
  - Contained documents mentioning a "Gentleman's Agreement"

# William Friedman Papers

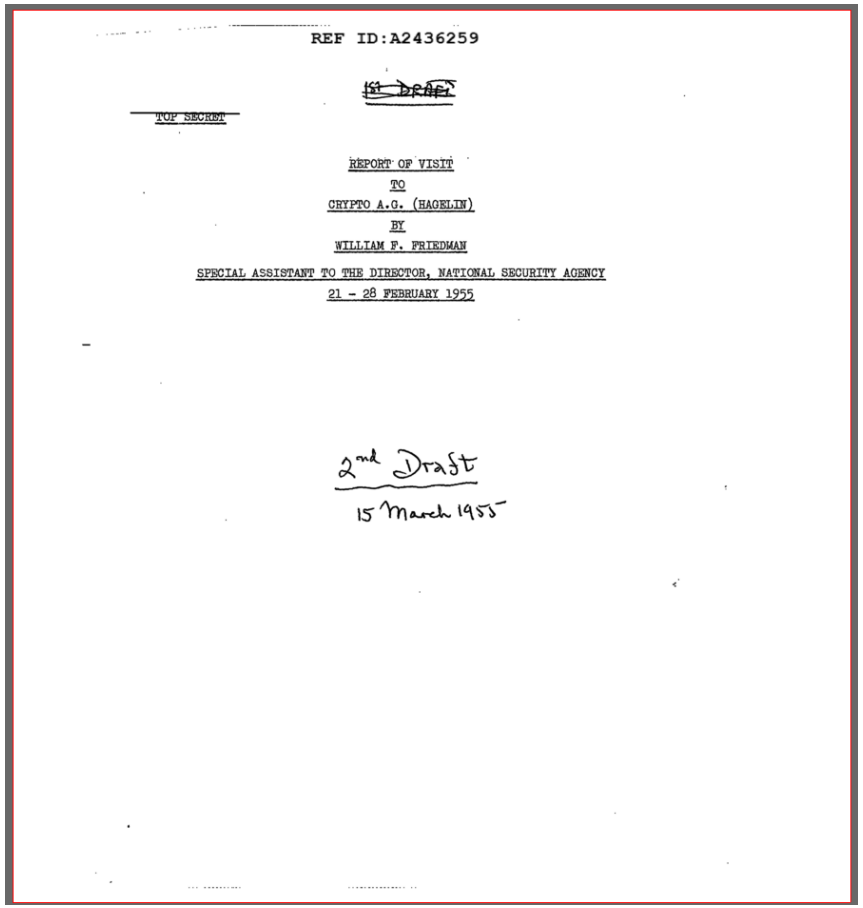
- NSA requested that the papers be “sequestered” in 1976
  - Library complied, but reopened files from 1979-1983
- An early reference to these papers appeared in James Bamford’s book, *The Puzzle Palace* (1982)
  - Bamford found references to the “Boris project”
  - Papers were again closed by the NSA in 1983
- In 2015, over 52,000 pages of this collection were redacted and released to the public
  - Papers are available online via the US National Archives



# Redaction Errors

- Process of reviewing and declassifying over 52,000 pages of material took NSA over two years
- Even though papers were over 50 years old, some information needed to remain secret to protect sources and methods
- Several cleared government officials were involved in the redaction process
  - Some papers had multiple copies
  - Those copies were not always reviewed and redacted by the same person

# Redacted Documents – Report of February, 1955 Visit (Cover Page)


REF ID:A2436259

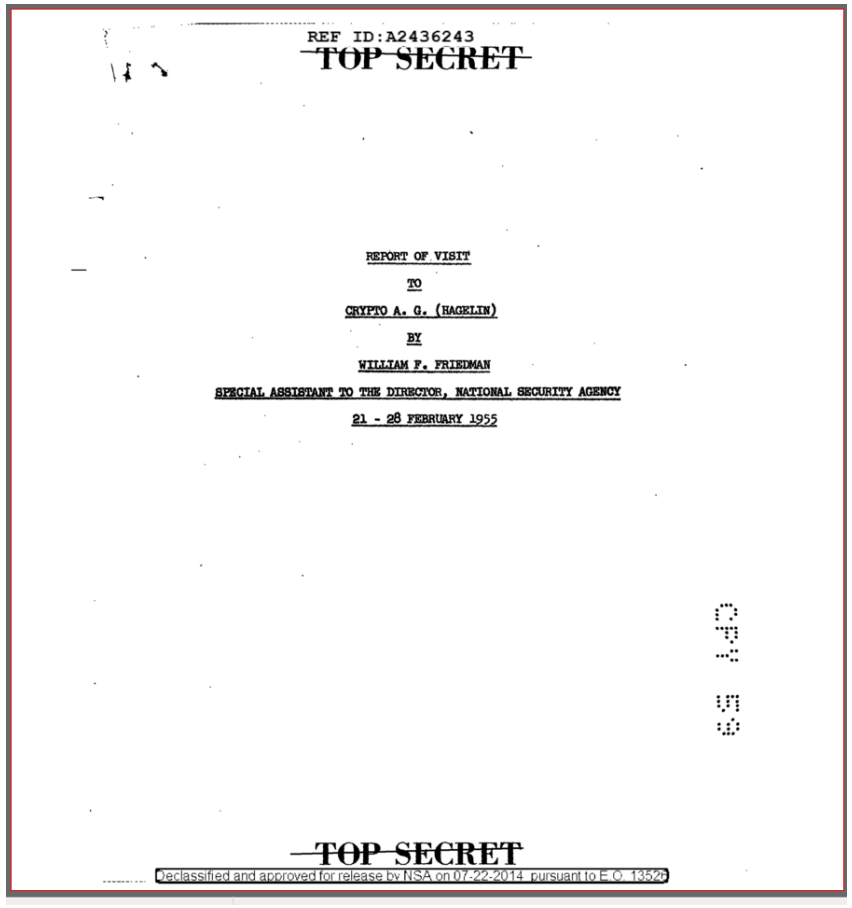
~~1st DRAFT~~

TOP SECRET

REPORT OF VISIT
TO
CRYPTO A.G. (HAGELIN)
BY
WILLIAM F. FRIEDMAN
SPECIAL ASSISTANT TO THE DIRECTOR, NATIONAL SECURITY AGENCY
21 - 28 FEBRUARY 1955

2nd Draft
15 March 1955

Redactor 1


REF ID:A2436243

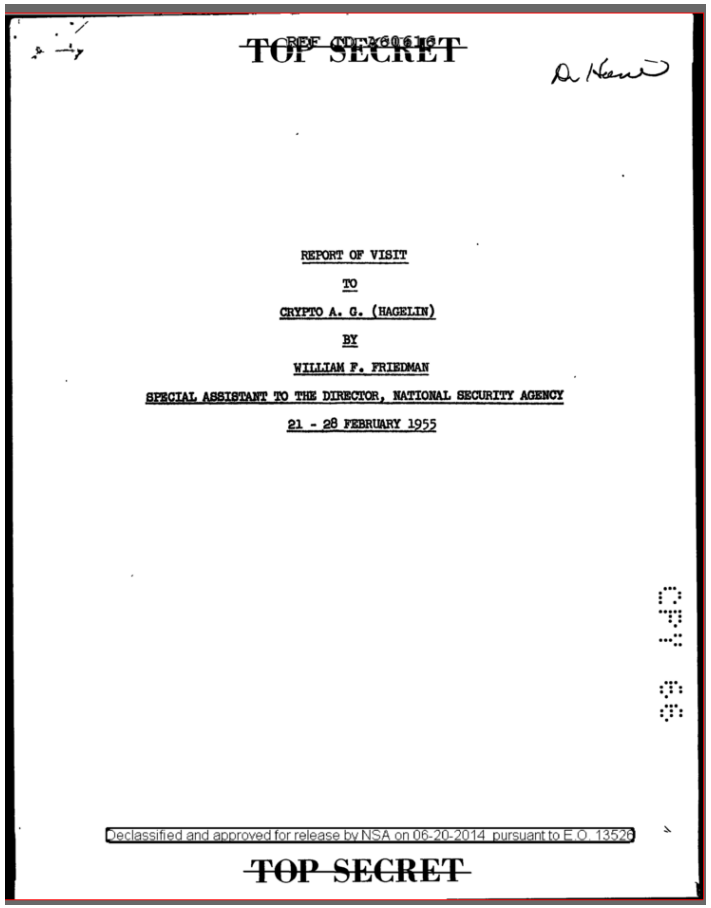
~~TOP SECRET~~

REPORT OF VISIT
TO
CRYPTO A. G. (HAGELIN)
BY
WILLIAM F. FRIEDMAN
SPECIAL ASSISTANT TO THE DIRECTOR, NATIONAL SECURITY AGENCY
21 - 28 FEBRUARY 1955

~~TOP SECRET~~

Declassified and approved for release by NSA on 07-22-2014 pursuant to E.O. 13526

Redactor 2


~~TOP SECRET~~

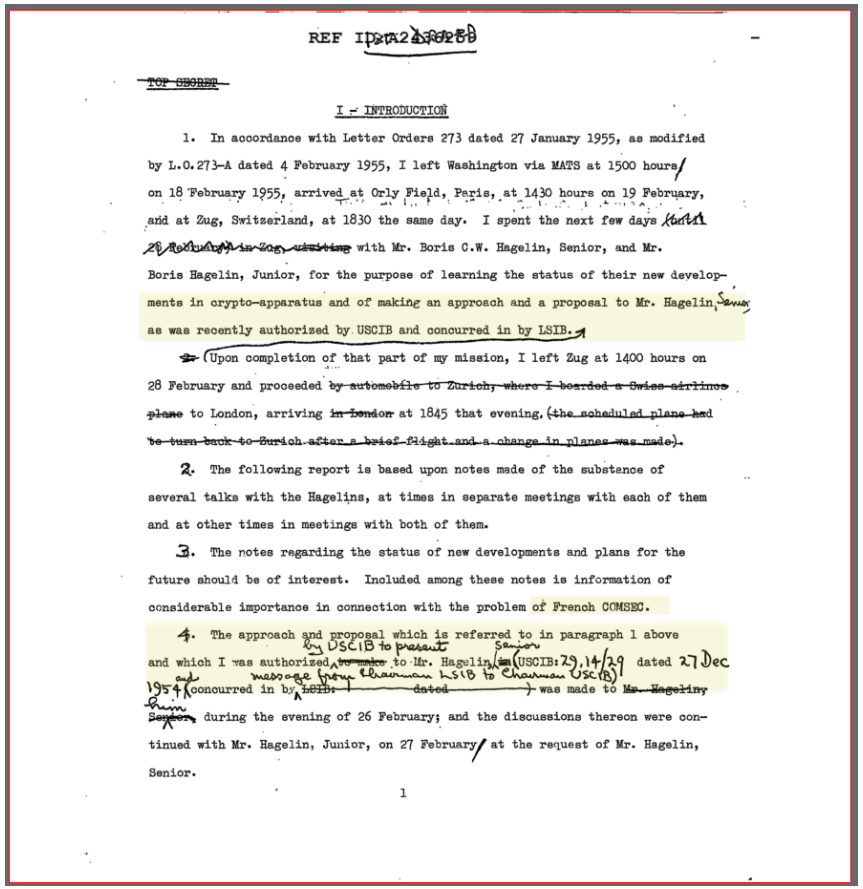
REPORT OF VISIT
TO
CRYPTO A. G. (HAGELIN)
BY
WILLIAM F. FRIEDMAN
SPECIAL ASSISTANT TO THE DIRECTOR, NATIONAL SECURITY AGENCY
21 - 28 FEBRUARY 1955

Declassified and approved for release by NSA on 06-20-2014 pursuant to E.O. 13526

~~TOP SECRET~~

Redactor 3

# Redacted Documents – Report of February, 1955 Visit (Example of un-redacted text)



REF ID:A2[redacted]

~~TOP SECRET~~

I - INTRODUCTION

1. In accordance with Letter Orders 273 dated 27 January 1955, as modified by L.O.273-A dated 4 February 1955, I left Washington via MATS at 1500 hours on 18 February 1955, arrived at Orly Field, Paris, at 1430 hours on 19 February, and at Zug, Switzerland, at 1830 the same day. I spent the next few days ~~(until 28 February in Zug, omitting~~ with Mr. Boris C.W. Hagelin, Senior, and Mr. Boris Hagelin, Junior, for the purpose of learning the status of their new developments in crypto-apparatus and of making an approach and a proposal to Mr. Hagelin, Senior as was recently authorized by USCIB and concurred in by LSIB.

~~2.~~ (Upon completion of that part of my mission, I left Zug at 1400 hours on 28 February and proceeded ~~by automobile to Zurich, where I boarded a Swiss airlines plane~~ to London, arriving ~~in London~~ at 1845 that evening, ~~(the scheduled plane had to turn back to Zurich after a brief flight and a change in planes was made).~~

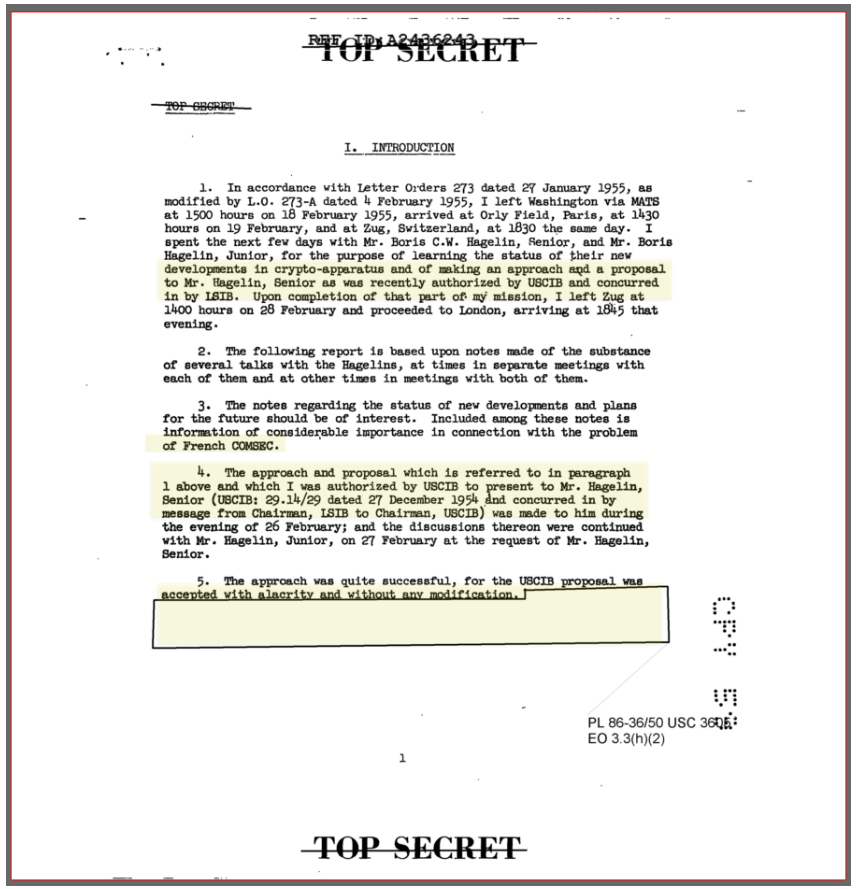
2. The following report is based upon notes made of the substance of several talks with the Hagelins, at times in separate meetings with each of them and at other times in meetings with both of them.

3. The notes regarding the status of new developments and plans for the future should be of interest. Included among these notes is information of considerable importance in connection with the problem of French COMSEC.

4. The approach and proposal which is referred to in paragraph 1 above and which I was authorized ~~to make~~ by USCIB to present to Mr. Hagelin, Senior (USCIB: 29.14/29 dated 27 Dec 1954 concurred in by ~~LSIB:~~ message from Chairman LSIB to Chairman USCIB) dated ~~was made to Mr. Hagelin, Senior,~~ during the evening of 26 February; and the discussions thereon were continued with Mr. Hagelin, Junior, on 27 February at the request of Mr. Hagelin, Senior.

1

Redactor 1



REF ID:A2436243

~~TOP SECRET~~

~~TOP SECRET~~

I. INTRODUCTION

1. In accordance with Letter Orders 273 dated 27 January 1955, as modified by L.O. 273-A dated 4 February 1955, I left Washington via MATS at 1500 hours on 18 February 1955, arrived at Orly Field, Paris, at 1430 hours on 19 February, and at Zug, Switzerland, at 1830 the same day. I spent the next few days with Mr. Boris C.W. Hagelin, Senior, and Mr. Boris Hagelin, Junior, for the purpose of learning the status of their new developments in crypto-apparatus and of making an approach and a proposal to Mr. Hagelin, Senior as was recently authorized by USCIB and concurred in by LSIB. Upon completion of that part of my mission, I left Zug at 1400 hours on 28 February and proceeded to London, arriving at 1845 that evening.

2. The following report is based upon notes made of the substance of several talks with the Hagelins, at times in separate meetings with each of them and at other times in meetings with both of them.

3. The notes regarding the status of new developments and plans for the future should be of interest. Included among these notes is information of considerable importance in connection with the problem of French COMSEC.

4. The approach and proposal which is referred to in paragraph 1 above and which I was authorized by USCIB to present to Mr. Hagelin, Senior (USCIB: 29.14/29 dated 27 December 1954 and concurred in by message from Chairman, LSIB to Chairman, USCIB) was made to him during the evening of 26 February; and the discussions thereon were continued with Mr. Hagelin, Junior, on 27 February at the request of Mr. Hagelin, Senior.

5. The approach was quite successful, for the USCIB proposal was accepted with alacrity and without any modification.

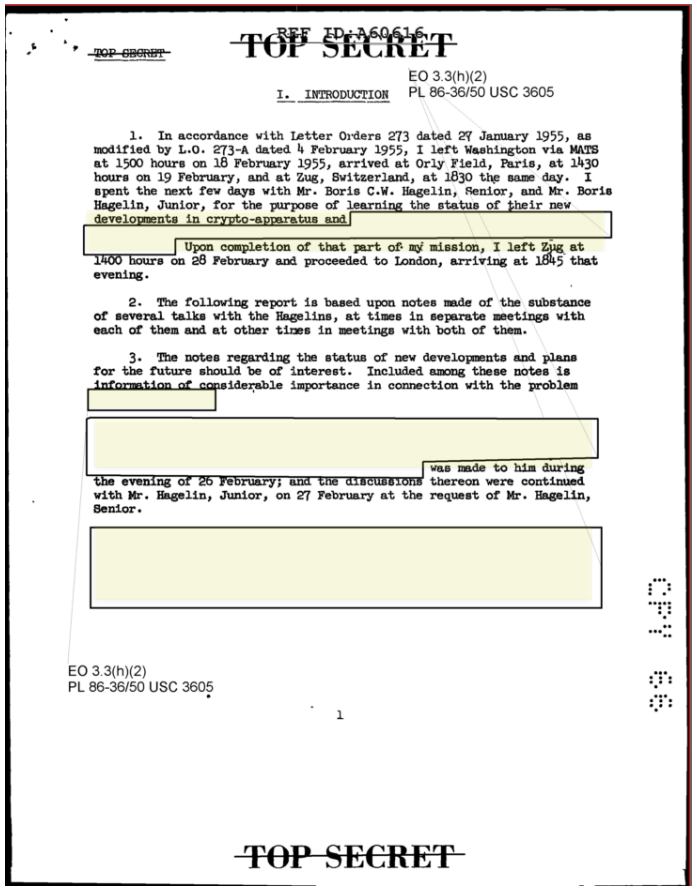
[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

1

~~TOP SECRET~~

Redactor 2



~~TOP SECRET~~

REF ID:A60616

~~TOP SECRET~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

I. INTRODUCTION

1. In accordance with Letter Orders 273 dated 27 January 1955, as modified by L.O. 273-A dated 4 February 1955, I left Washington via MATS at 1500 hours on 18 February 1955, arrived at Orly Field, Paris, at 1430 hours on 19 February, and at Zug, Switzerland, at 1830 the same day. I spent the next few days with Mr. Boris C.W. Hagelin, Senior, and Mr. Boris Hagelin, Junior, for the purpose of learning the status of their new developments in crypto-apparatus and [redacted]

Upon completion of that part of my mission, I left Zug at 1400 hours on 28 February and proceeded to London, arriving at 1845 that evening.

2. The following report is based upon notes made of the substance of several talks with the Hagelins, at times in separate meetings with each of them and at other times in meetings with both of them.

3. The notes regarding the status of new developments and plans for the future should be of interest. Included among these notes is information of considerable importance in connection with the problem [redacted]

[redacted] was made to him during the evening of 26 February; and the discussions thereon were continued with Mr. Hagelin, Junior, on 27 February at the request of Mr. Hagelin, Senior.

[redacted]

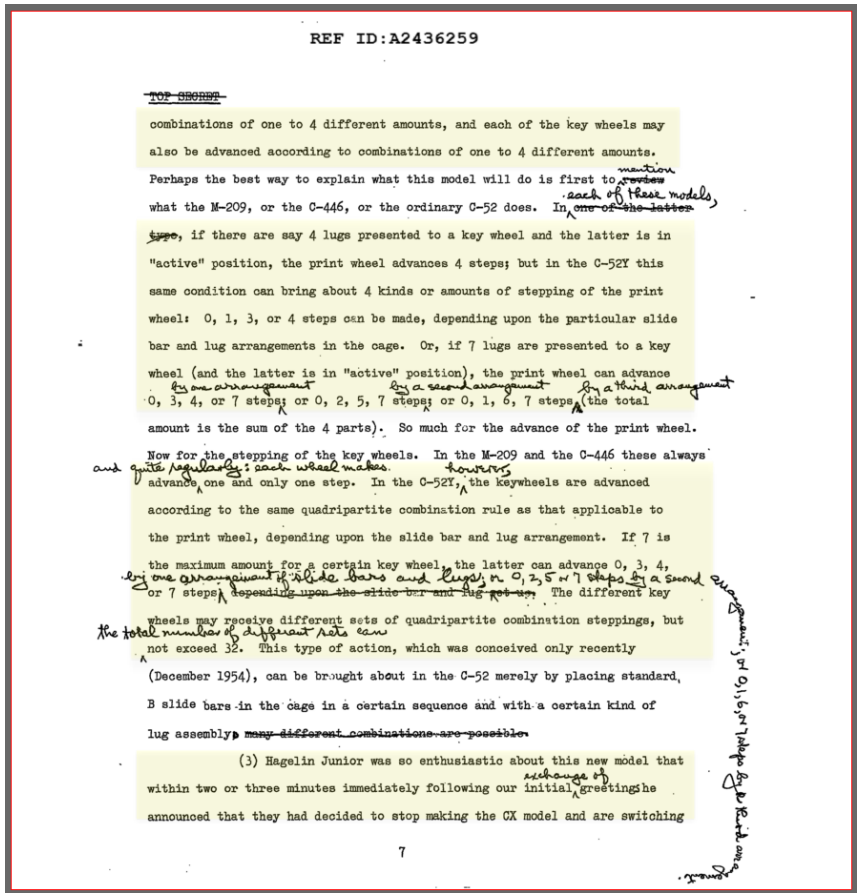
EO 3.3(h)(2)
PL 86-36/50 USC 3605

1

~~TOP SECRET~~

Redactor 3

# Redacted Documents – Report of February, 1955 Visit (Example of fully un-redacted text)



REF ID:A2436259

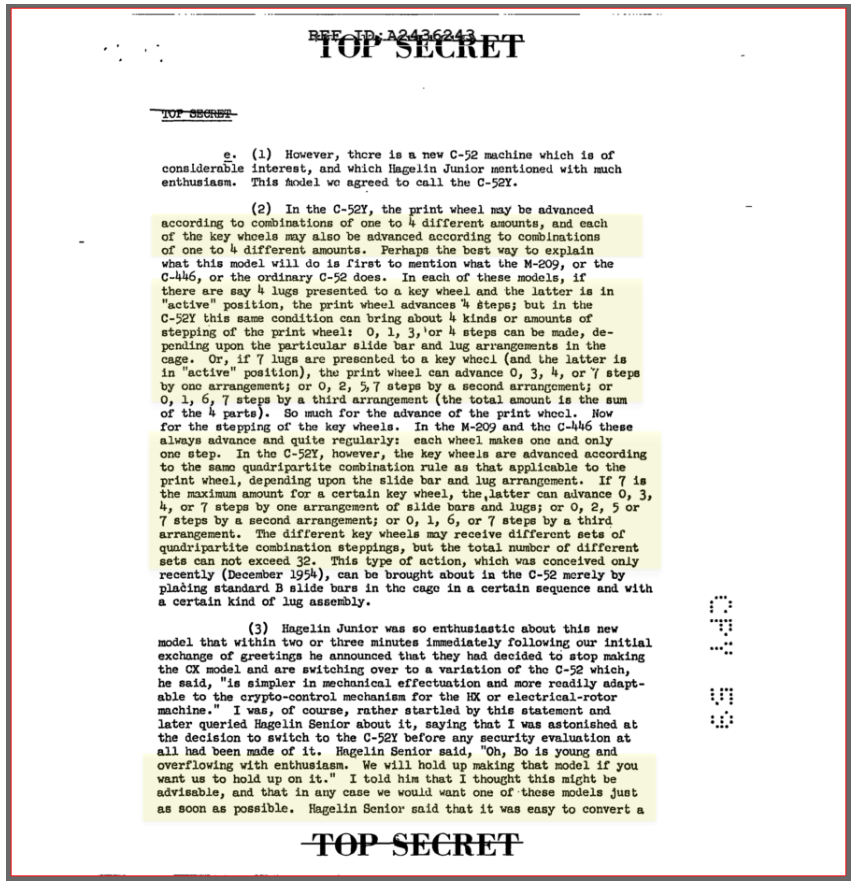
~~TOP SECRET~~

combinations of one to 4 different amounts, and each of the key wheels may also be advanced according to combinations of one to 4 different amounts. Perhaps the best way to explain what this model will do is first to ~~review~~ mention what the M-209, or the C-446, or the ordinary C-52 does. In ~~one of the latter~~ each of these models, ~~type~~, if there are say 4 lugs presented to a key wheel and the latter is in "active" position, the print wheel advances 4 steps; but in the C-52Y this same condition can bring about 4 kinds or amounts of stepping of the print wheel: 0, 1, 3, or 4 steps can be made, depending upon the particular slide bar and lug arrangements in the cage. Or, if 7 lugs are presented to a key wheel (and the latter is in "active" position), the print wheel can advance 0, 3, 4, or 7 steps by one arrangement; or 0, 2, 5, 7 steps by a second arrangement; or 0, 1, 6, 7 steps by a third arrangement (the total amount is the sum of the 4 parts). So much for the advance of the print wheel. Now for the stepping of the key wheels. In the M-209 and the C-446 these always and quite regularly: each wheel makes one and only one step. In the C-52Y, however, the keywheels are advanced according to the same quadripartite combination rule as that applicable to the print wheel, depending upon the slide bar and lug arrangement. If 7 is the maximum amount for a certain key wheel, the latter can advance 0, 3, 4, or 7 steps ~~depending upon the slide bar and lug set up~~. The different key wheels may receive different sets of quadripartite combination steppings, but the total number of different sets can not exceed 32. This type of action, which was conceived only recently (December 1954), can be brought about in the C-52 merely by placing standard B slide bars in the cage in a certain sequence and with a certain kind of lug assembly. ~~many different combinations are possible.~~

(3) Hagelin Junior was so enthusiastic about this new model that within two or three minutes immediately following our initial exchange of greetings he announced that they had decided to stop making the CX model and are switching

7

Redactor 1



~~TOP SECRET~~

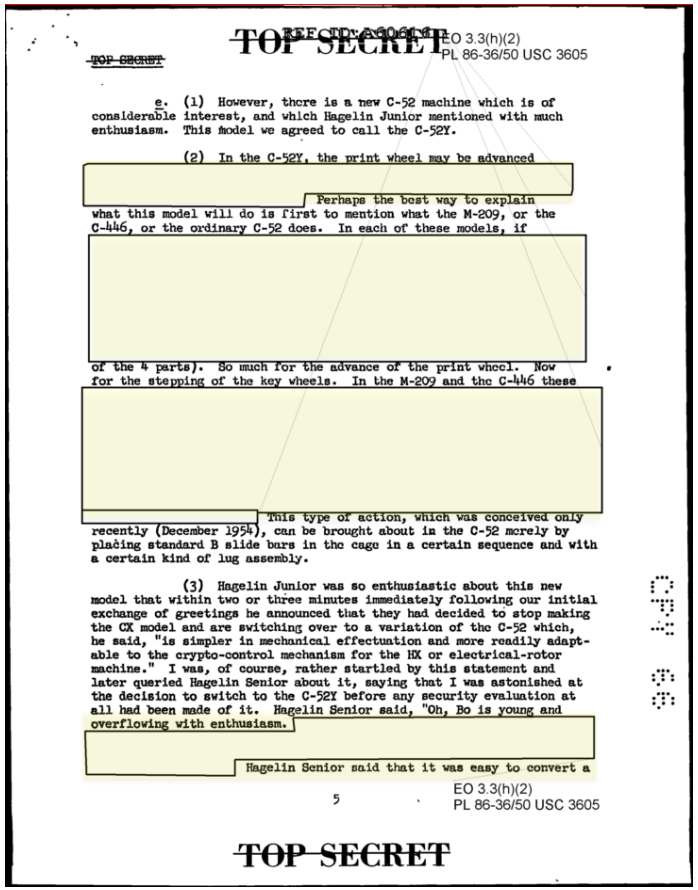
e. (1) However, there is a new C-52 machine which is of considerable interest, and which Hagelin Junior mentioned with much enthusiasm. This model we agreed to call the C-52Y.

(2) In the C-52Y, the print wheel may be advanced according to combinations of one to 4 different amounts, and each of the key wheels may also be advanced according to combinations of one to 4 different amounts. Perhaps the best way to explain what this model will do is first to mention what the M-209, or the C-446, or the ordinary C-52 does. In each of these models, if there are say 4 lugs presented to a key wheel and the latter is in "active" position, the print wheel advances 4 steps; but in the C-52Y this same condition can bring about 4 kinds or amounts of stepping of the print wheel: 0, 1, 3, or 4 steps can be made, depending upon the particular slide bar and lug arrangements in the cage. Or, if 7 lugs are presented to a key wheel (and the latter is in "active" position), the print wheel can advance 0, 3, 4, or 7 steps by one arrangement; or 0, 2, 5, 7 steps by a second arrangement; or 0, 1, 6, 7 steps by a third arrangement (the total amount is the sum of the 4 parts). So much for the advance of the print wheel. Now for the stepping of the key wheels. In the M-209 and the C-446 these always advance and quite regularly: each wheel makes one and only one step. In the C-52Y, however, the key wheels are advanced according to the same quadripartite combination rule as that applicable to the print wheel, depending upon the slide bar and lug arrangement. If 7 is the maximum amount for a certain key wheel, the latter can advance 0, 3, 4, or 7 steps by one arrangement of slide bars and lugs; or 0, 2, 5 or 7 steps by a second arrangement; or 0, 1, 6, or 7 steps by a third arrangement. The different key wheels may receive different sets of quadripartite combination steppings, but the total number of different sets can not exceed 32. This type of action, which was conceived only recently (December 1954), can be brought about in the C-52 merely by placing standard B slide bars in the cage in a certain sequence and with a certain kind of lug assembly.

(3) Hagelin Junior was so enthusiastic about this new model that within two or three minutes immediately following our initial exchange of greetings he announced that they had decided to stop making the CX model and are switching over to a variation of the C-52 which, he said, "is simpler in mechanical effectuation and more readily adaptable to the crypto-control mechanism for the HX or electrical-rotor machine." I was, of course, rather startled by this statement and later queried Hagelin Senior about it, saying that I was astonished at the decision to switch to the C-52Y before any security evaluation at all had been made of it. Hagelin Senior said, "Oh, Bo is young and overflowing with enthusiasm. We will hold up making that model if you want us to hold up on it." I told him that I thought this might be advisable, and that in any case we would want one of these models just as soon as possible. Hagelin Senior said that it was easy to convert a

~~TOP SECRET~~

Redactor 2



~~TOP SECRET~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET~~

e. (1) However, there is a new C-52 machine which is of considerable interest, and which Hagelin Junior mentioned with much enthusiasm. This model we agreed to call the C-52Y.

(2) In the C-52Y, the print wheel may be advanced

Perhaps the best way to explain what this model will do is first to mention what the M-209, or the C-446, or the ordinary C-52 does. In each of these models, if

of the 4 parts). So much for the advance of the print wheel. Now for the stepping of the key wheels. In the M-209 and the C-446 these

This type of action, which was conceived only recently (December 1954), can be brought about in the C-52 merely by placing standard B slide bars in the cage in a certain sequence and with a certain kind of lug assembly.

(3) Hagelin Junior was so enthusiastic about this new model that within two or three minutes immediately following our initial exchange of greetings he announced that they had decided to stop making the CX model and are switching over to a variation of the C-52 which, he said, "is simpler in mechanical effectuation and more readily adaptable to the crypto-control mechanism for the HX or electrical-rotor machine." I was, of course, rather startled by this statement and later queried Hagelin Senior about it, saying that I was astonished at the decision to switch to the C-52Y before any security evaluation at all had been made of it. Hagelin Senior said, "Oh, Bo is young and overflowing with enthusiasm.

Hagelin Senior said that it was easy to convert a

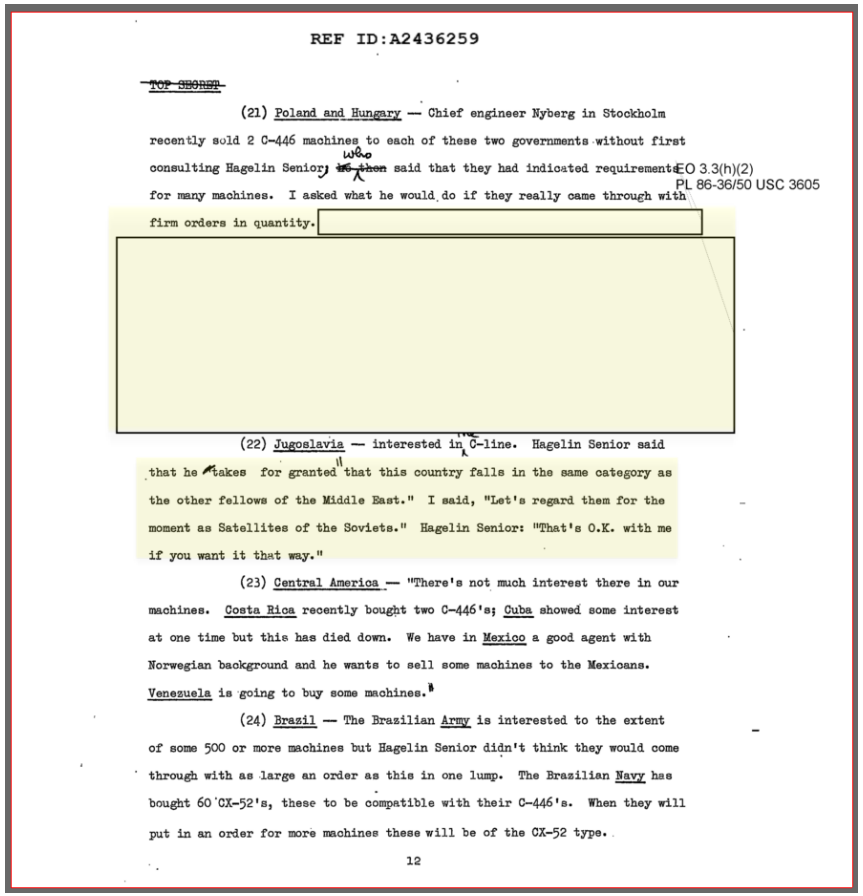
5

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET~~

Redactor 3

# Redacted Documents – Report of February, 1955 Visit (Example of partially un-redacted text)



REF ID:A2436259

~~TOP SECRET~~

(21) Poland and Hungary — Chief engineer Nyberg in Stockholm recently sold 2 C-446 machines to each of these two governments without first consulting Hagelin Senior; ~~he then~~ said that they had indicated requirements for many machines. I asked what he would do if they really came through with firm orders in quantity. [redacted] EO 3.3(h)(2) PL 86-36/50 USC 3605

[redacted]

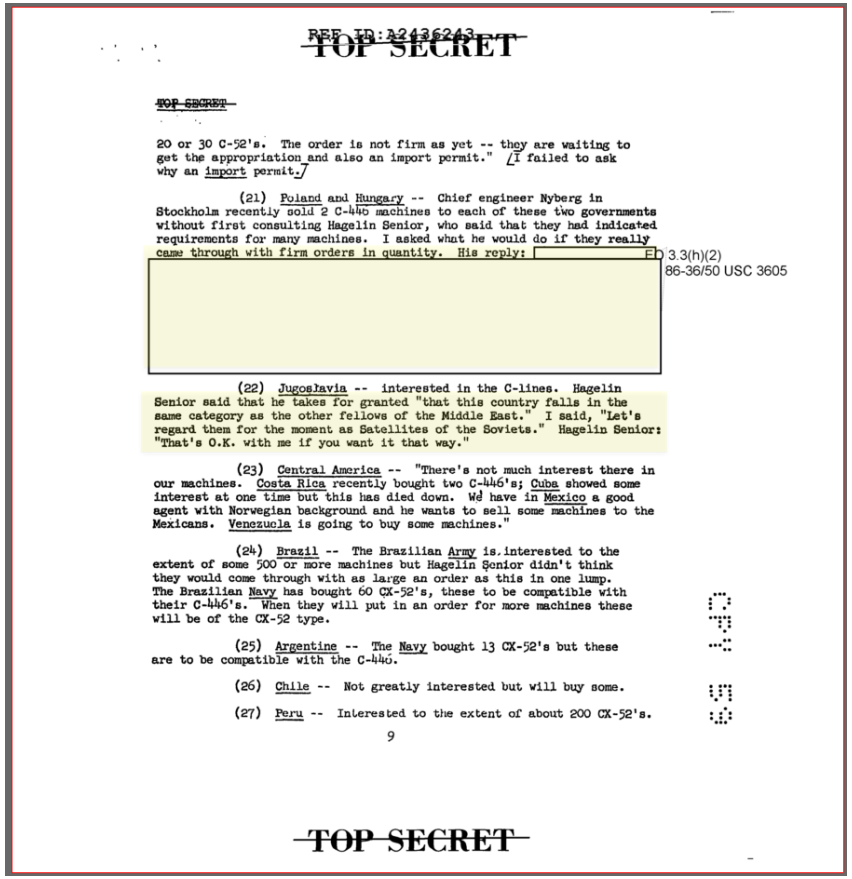
(22) Jugoslavia — interested in C-line. Hagelin Senior said that he takes for granted that this country falls in the same category as the other fellows of the Middle East." I said, "Let's regard them for the moment as Satellites of the Soviets." Hagelin Senior: "That's O.K. with me if you want it that way."

(23) Central America — "There's not much interest there in our machines. Costa Rica recently bought two C-446's; Cuba showed some interest at one time but this has died down. We have in Mexico a good agent with Norwegian background and he wants to sell some machines to the Mexicans. Venezuela is going to buy some machines."

(24) Brazil — The Brazilian Army is interested to the extent of some 500 or more machines but Hagelin Senior didn't think they would come through with as large an order as this in one lump. The Brazilian Navy has bought 60 CX-52's, these to be compatible with their C-446's. When they will put in an order for more machines these will be of the CX-52 type.

12

Redactor 1



~~TOP SECRET~~

~~TOP SECRET~~

20 or 30 C-52's. The order is not firm as yet -- they are waiting to get the appropriation and also an import permit." I failed to ask why an import permit.

(21) Poland and Hungary -- Chief engineer Nyberg in Stockholm recently sold 2 C-446 machines to each of these two governments without first consulting Hagelin Senior, who said that they had indicated requirements for many machines. I asked what he would do if they really came through with firm orders in quantity. His reply: [redacted] EO 3.3(h)(2) 86-36/50 USC 3605

[redacted]

(22) Jugoslavia -- interested in the C-lines. Hagelin Senior said that he takes for granted "that this country falls in the same category as the other fellows of the Middle East." I said, "Let's regard them for the moment as Satellites of the Soviets." Hagelin Senior: "That's O.K. with me if you want it that way."

(23) Central America -- "There's not much interest there in our machines. Costa Rica recently bought two C-446's; Cuba showed some interest at one time but this has died down. We have in Mexico a good agent with Norwegian background and he wants to sell some machines to the Mexicans. Venezuela is going to buy some machines."

(24) Brazil -- The Brazilian Army is interested to the extent of some 500 or more machines but Hagelin Senior didn't think they would come through with as large an order as this in one lump. The Brazilian Navy has bought 60 CX-52's, these to be compatible with their C-446's. When they will put in an order for more machines these will be of the CX-52 type.

(25) Argentine -- The Navy bought 13 CX-52's but these are to be compatible with the C-446.

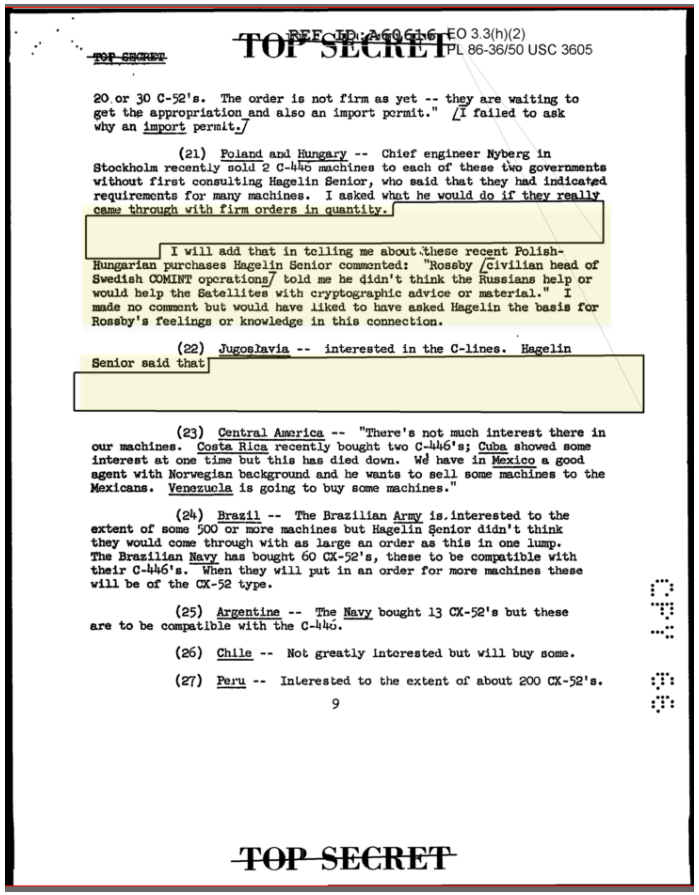
(26) Chile -- Not greatly interested but will buy some.

(27) Peru -- Interested to the extent of about 200 CX-52's.

9

~~TOP SECRET~~

Redactor 2



~~TOP SECRET~~ ~~TOP SECRET~~ EO 3.3(h)(2) PL 86-36/50 USC 3605

20 or 30 C-52's. The order is not firm as yet -- they are waiting to get the appropriation and also an import permit." I failed to ask why an import permit.

(21) Poland and Hungary -- Chief engineer Nyberg in Stockholm recently sold 2 C-446 machines to each of these two governments without first consulting Hagelin Senior, who said that they had indicated requirements for many machines. I asked what he would do if they really came through with firm orders in quantity.

[redacted]

I will add that in telling me about these recent Polish-Hungarian purchases Hagelin Senior commented: "Rossby civilian head of Swedish COMINT operations told me he didn't think the Russians help or would help the Satellites with cryptographic advice or material." I made no comment but would have liked to have asked Hagelin the basis for Rossby's feelings or knowledge in this connection.

(22) Jugoslavia -- interested in the C-lines. Hagelin Senior said that [redacted]

(23) Central America -- "There's not much interest there in our machines. Costa Rica recently bought two C-446's; Cuba showed some interest at one time but this has died down. We have in Mexico a good agent with Norwegian background and he wants to sell some machines to the Mexicans. Venezuela is going to buy some machines."

(24) Brazil -- The Brazilian Army is interested to the extent of some 500 or more machines but Hagelin Senior didn't think they would come through with as large an order as this in one lump. The Brazilian Navy has bought 60 CX-52's, these to be compatible with their C-446's. When they will put in an order for more machines these will be of the CX-52 type.

(25) Argentine -- The Navy bought 13 CX-52's but these are to be compatible with the C-446.

(26) Chile -- Not greatly interested but will buy some.

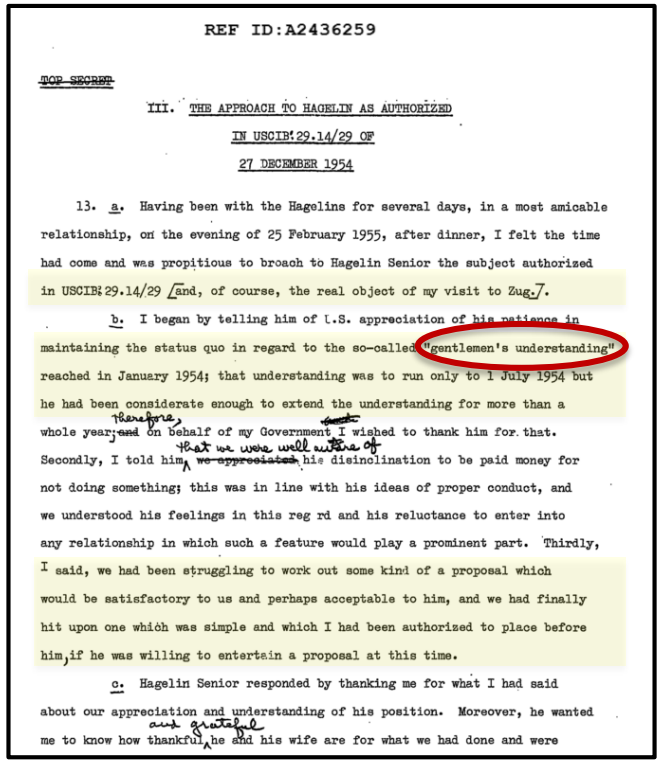
(27) Peru -- Interested to the extent of about 200 CX-52's.

9

~~TOP SECRET~~

Redactor 3

# Redacted Documents – Report of February, 1955 Visit (First mention of a "gentlemen's understanding")



REF ID:A2436259

~~TOP SECRET~~

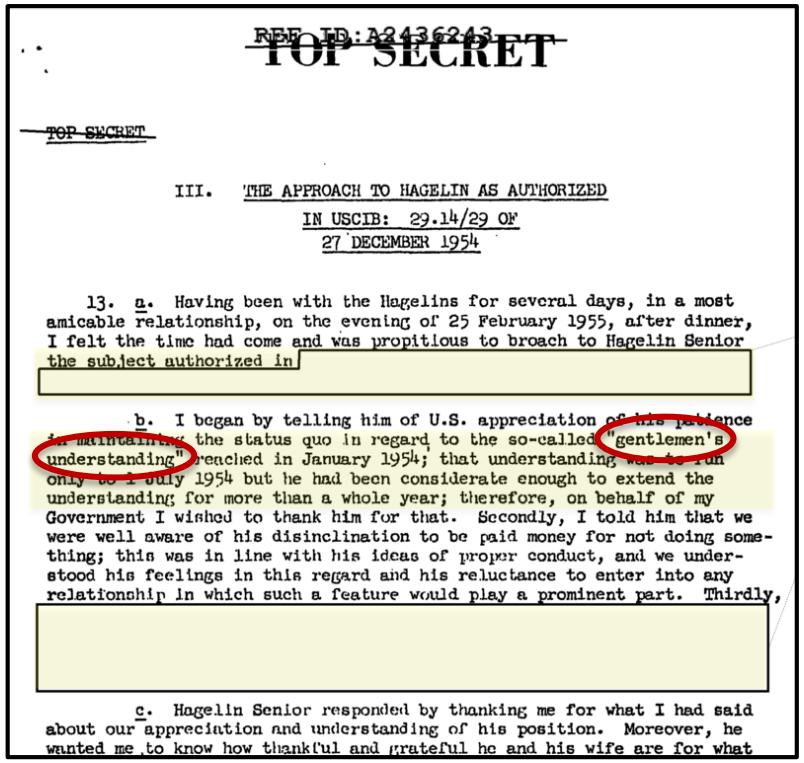
III. THE APPROACH TO HAGELIN AS AUTHORIZED
IN USCIB: 29.14/29 OF
27 DECEMBER 1954

13. a. Having been with the Hagelins for several days, in a most amicable relationship, on the evening of 25 February 1955, after dinner, I felt the time had come and was propitious to broach to Hagelin Senior the subject authorized in USCIB: 29.14/29 and, of course, the real object of my visit to Zug.

b. I began by telling him of U.S. appreciation of his patience in maintaining the status quo in regard to the so-called "gentlemen's understanding" reached in January 1954; that understanding was to run only to 1 July 1954 but he had been considerate enough to extend the understanding for more than a whole year; therefore, on behalf of my Government I wished to thank him for that. Secondly, I told him that we were well aware of his disinclination to be paid money for not doing something; this was in line with his ideas of proper conduct, and we understood his feelings in this reg rd and his reluctance to enter into any relationship in which such a feature would play a prominent part. Thirdly, I said, we had been struggling to work out some kind of a proposal which would be satisfactory to us and perhaps acceptable to him, and we had finally hit upon one which was simple and which I had been authorized to place before him, if he was willing to entertain a proposal at this time.

c. Hagelin Senior responded by thanking me for what I had said about our appreciation and understanding of his position. Moreover, he wanted me to know how thankful and grateful he and his wife are for what we had done and were

Redactor 1



~~REF ID:A2436243~~

~~TOP SECRET~~

~~TOP SECRET~~

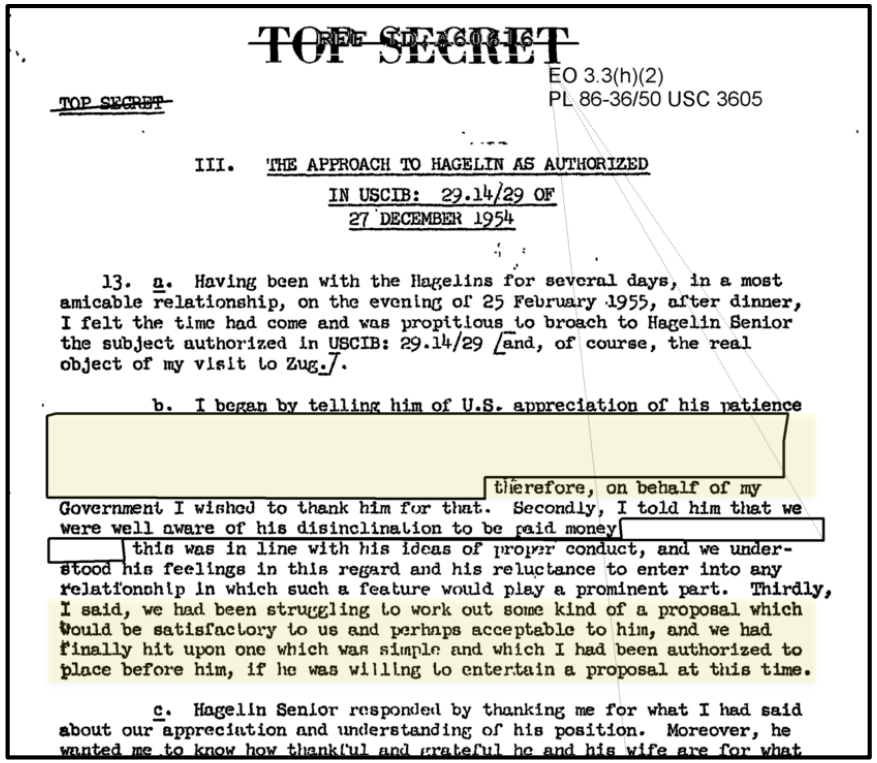
III. THE APPROACH TO HAGELIN AS AUTHORIZED
IN USCIB: 29.14/29 OF
27 DECEMBER 1954

13. a. Having been with the Hagelins for several days, in a most amicable relationship, on the evening of 25 February 1955, after dinner, I felt the time had come and was propitious to broach to Hagelin Senior the subject authorized in [redacted]

b. I began by telling him of U.S. appreciation of his patience in maintaining the status quo in regard to the so-called "gentlemen's understanding" reached in January 1954; that understanding was to run only to 1 July 1954 but he had been considerate enough to extend the understanding for more than a whole year; therefore, on behalf of my Government I wished to thank him for that. Secondly, I told him that we were well aware of his disinclination to be paid money for not doing something; this was in line with his ideas of proper conduct, and we understood his feelings in this regard and his reluctance to enter into any relationship in which such a feature would play a prominent part. Thirdly, [redacted]

c. Hagelin Senior responded by thanking me for what I had said about our appreciation and understanding of his position. Moreover, he wanted me to know how thankful and grateful he and his wife are for what

Redactor 2



~~TOP SECRET~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET~~

III. THE APPROACH TO HAGELIN AS AUTHORIZED
IN USCIB: 29.14/29 OF
27 DECEMBER 1954

13. a. Having been with the Hagelins for several days, in a most amicable relationship, on the evening of 25 February 1955, after dinner, I felt the time had come and was propitious to broach to Hagelin Senior the subject authorized in USCIB: 29.14/29 and, of course, the real object of my visit to Zug.

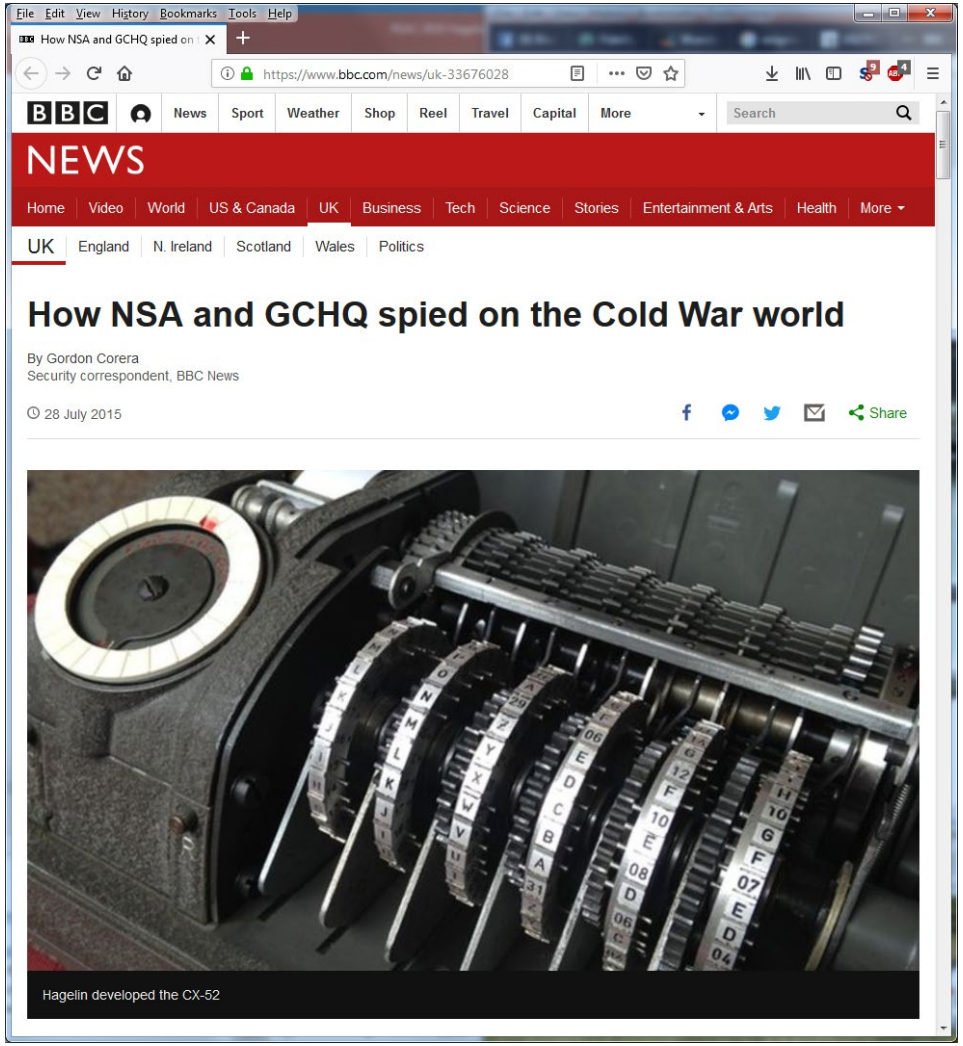
b. I began by telling him of U.S. appreciation of his patience [redacted] therefore, on behalf of my Government I wished to thank him for that. Secondly, I told him that we were well aware of his disinclination to be paid money [redacted] this was in line with his ideas of proper conduct, and we understood his feelings in this regard and his reluctance to enter into any relationship in which such a feature would play a prominent part. Thirdly, I said, we had been struggling to work out some kind of a proposal which would be satisfactory to us and perhaps acceptable to him, and we had finally hit upon one which was simple and which I had been authorized to place before him, if he was willing to entertain a proposal at this time.

c. Hagelin Senior responded by thanking me for what I had said about our appreciation and understanding of his position. Moreover, he wanted me to know how thankful and grateful he and his wife are for what

Redactor 3

USCIB = United States Communications Intelligence Board

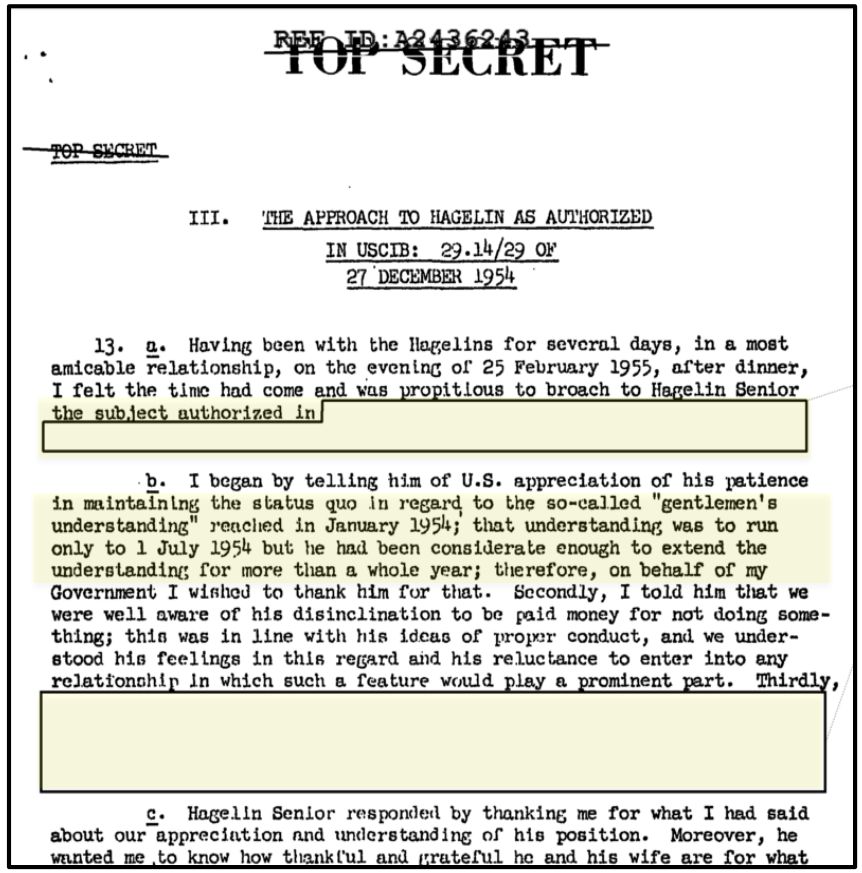
# BBC Story On Friedman And Hagelin




- Papers declassified and put online in April, 2015
- BBC story in July 2015 highlighted redaction mistakes
- Rejuvenated an old rumor that NSA and GCHQ had secretly worked with Crypto AG to develop “weaker” devices for non-NATO countries

# Friedman and Hagelin's "Gentleman's Understanding"

- New Hagelin machines, in particular the CX-52 and the forthcoming TC-55 (teletype encryption) were of serious concern to the NSA, due to "insolvability"
- Friedman communicated with Hagelin using private stationary and his home address about the situation to avoid the delivery of NSA letters to a small town
- Friedman and Hagelin agreed to a "gentleman's understanding" that Crypto AG would not sell the new devices until NSA could develop new guidance



~~REF ID: A2436243~~ ~~TOP SECRET~~

~~TOP SECRET~~

III. THE APPROACH TO HAGELIN AS AUTHORIZED IN USCIB: 29.14/29 OF 27 DECEMBER 1954

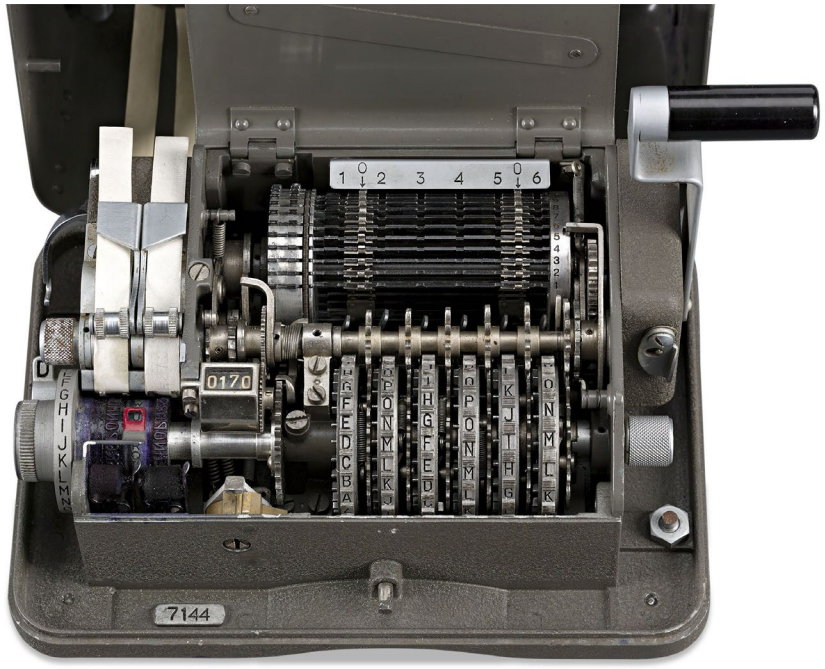
13. a. Having been with the Hagelins for several days, in a most amicable relationship, on the evening of 25 February 1955, after dinner, I felt the time had come and was propitious to broach to Hagelin Senior the subject authorized in

b. I began by telling him of U.S. appreciation of his patience in maintaining the status quo in regard to the so-called "gentlemen's understanding" reached in January 1954; that understanding was to run only to 1 July 1954 but he had been considerate enough to extend the understanding for more than a whole year; therefore, on behalf of my Government I wished to thank him for that. Secondly, I told him that we were well aware of his disinclination to be paid money for not doing something; this was in line with his ideas of proper conduct, and we understood his feelings in this regard and his reluctance to enter into any relationship in which such a feature would play a prominent part. Thirdly,

c. Hagelin Senior responded by thanking me for what I had said about our appreciation and understanding of his position. Moreover, he wanted me to know how thankful and grateful he and his wife are for what

# Old vs New Crypto AG Machines – Six Month Agreement

M-209/C-38
***OK** to sell to non-NATO*




C-446
***OK** to sell to non-NATO*

CX-52
***Not OK** to sell to non-NATO*

# A Gentleman's Understanding Becomes A Formal Arrangement - 1955

- Original understanding was for a six-month delay of sales (January to July, 1954) but was still in effect in February 1955
- New proposal was for NSA to develop instructions for NATO countries that would be different from instructions for non-NATO countries for the new machines
  - NATO instructions would ensure that very strong encryption was used
  - Non-NATO instructions would result in the devices producing weakened encryption
  - Crypto AG would not have access to the NATO instructions
  - Crypto AG could sell devices to any country, NSA would provide separate operating instructions to NATO users

# Agreement Summary

- Crypto AG continues to sell C-446 and C-52 to countries Hagelin felt should have their messages intercepted and read
  - Crypto AG would inform NSA and GCHQ about technical specs of the machines and which versions were sold to which countries
- Crypto AG sells CX-52, TC-55, etc. to “friendly” countries
  - All customers receive Crypto AG instructions that, if followed, result in a weaker system
  - NATO countries provided with classified instructions (“brochures”) for much stronger encryption using the same machines
- Hagelin allowed to sell his machines in the US with no import/export restrictions
- Hagelin’s son-in-law had his active duty status in the US Air Force retained and a cousin of Hagelin's wife was employed by the NSA

# Revelation Of “Backdoor” To Israel And Iran

- Secret deal disclosed to Israel by spy Jonathan Pollard in 1983
- Israel passed Hagelin information to Russia in exchange for increase in Soviet Jewish refugees
- Soviets already knew about the arrangement from spies Aldrich Ames and Robert Hanssen, and likely told Iran about the backdoor
- Former Iranian Prime Minister Shahpour Baktiar assassinated in 1991
- The day of the assassination, but before his body was found, US decoded a message to Iranian embassies, "Is Bakhtiar dead?"

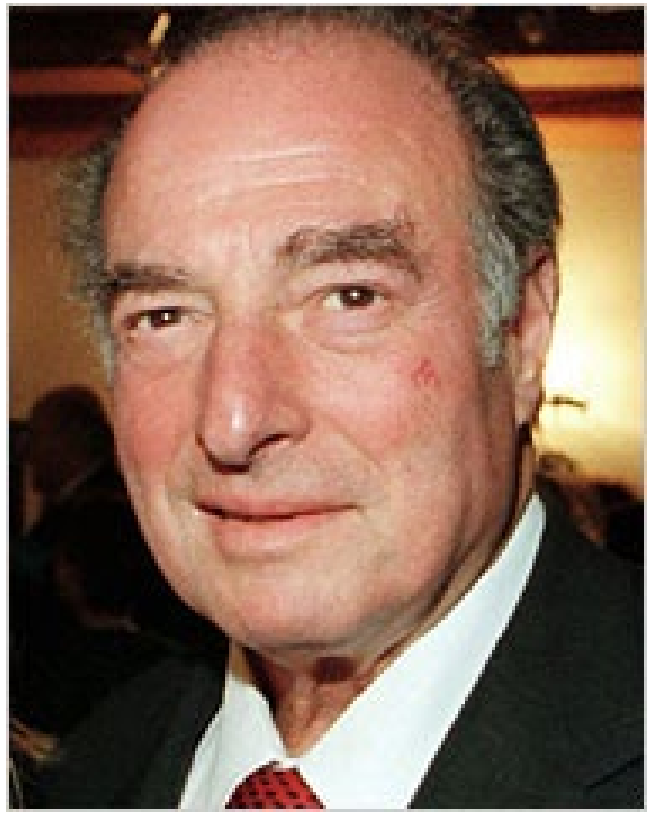
# Iranian Kidnapping Of Hans Bühler - 1992

Hans Bühler
(1941-2017)

- In 1992, Iran kidnapped Crypto salesman Hans Buehler, accused of spying for US/Germany
- Buehler interrogated five hours per day for nine months but had no knowledge of the weaker Crypto AG devices
- Crypto AG and Siemens paid the million dollar ransom
- Buehler wrote a book about his ordeal and discoveries
  - Available online as a free PDF
- Boris Hagelin admits existence of special arrangement to Hagelin engineer, but Crypto AG denies it
- 2015 release of Friedman papers confirmed the rumors

# The Rest Of The Story

- Accusation of the NSA deal by Iran caused Crypto AG sales and stock value to plummet
- Faced with bankruptcy, Crypto AG was saved by angel investor Marc Rich
- Rich was a resident of Zug and a fugitive billionaire with ties to Israel's Mossad
- Speculated he used the agreement information for financial gain and to aid Israeli intelligence
- Clinton pardoned Rich in his last hours in the White House, January 2001
  - Rich's attorney was Scooter Libby, later Cheney's Chief of Staff, who outted CIA agent Valerie Plame and was later convicted of four felonies (Libby was pardoned by Trump in April 2018)



Marc Rich
(1934-2013)

# Apply What You Have Learned Today

- Next week you should:
  - Review information you have made public that might be sensitive
- In the first three months following this presentation you should:
  - Verify the source and trustworthiness of your technology providers
  - Define appropriate controls for future purchases
- Within six months you should:
  - Verify that any dependencies you have on encryption use publicly recognized algorithms, and not privately developed ones
  - Read a book on security history and apply what you learned

# Credits and References

Many thanks to the following websites for images, diagrams, and historical information:

- archives.gov
- bbc.co.uk
- cryptomuseum.com
- ciphermachines.com
- nf6x.net
- nsa.gov
- users.telenet.be

BORIS HAGELIN.
Famous Swedish Inventor.
Creator of the World War II
German coding machine.
Universal Pictorial Press
photo (P 394242) Jun 1980.