

paid by [redacted] and commented on by H. Schorrack. (This was rewritten by H. Schorrack)

Boris Caesar Wilhelm Hagelin was born in southern Russia ^{K.W. HAGELIN,} in 1892. His father was employed by the Nobel brothers as manager of their oil fields and refineries, ^{and} and during his ^{at one} life became an investor in, and consul-general of A. B. ^{A.B. Cryptograph at one time in a Swedish in St. Petersburg (X)} time he was the Swedish Consul-General in St. Petersburg; he was also an investor in the A. B. Cryptograph Company.

A. B. Cryptograph was started in Stockholm for the purpose of developing and marketing inventions and ciphering machines made by the Swedish engineer A. G. Damm. It was expected that this equipment would be used in military and diplomatic applications. ³ (X)

was it? If so - say so.

Boris Hagelin, who lived ^{and} and obtained his higher education ^{there,} in Sweden joined A. B. Cryptograph in 1922. Hagelin held a degree in Mechanical Engineering from the Royal Institute of Technology in Stockholm. The practical experience Hagelin brought to ~~the firm~~ A. B. Cryptograph included six years employment with ASEA (Sweden's General Electric) and one year with Standard Oil in the United States. ⁴ (X)

~~Through his work,~~ ^{Upon learning,} Hagelin discovered that the Swedish military was considering the purchase of a German Enigma machine, ~~Boris Hagelin~~ modified ^{and improved} one of the firm's equipments (probably the B1, a problem-riddled cipher machine), ~~thus~~ putting it into competition with the Enigma. He offered this device, designated B-21, to the

Swedish Army, which subsequently placed a sizeable order in 1926. (S)

The U.S. Army was also becoming aware of Hagelin's machines. Their interest resulted from the development in Europe of more than one series of mechanical and electro-mechanical ciphering devices comparable to the Hebern machine. The rotor principle had been developed not only by Arthur Scherbius (Enigma), but also by Mr. Damm ^{whose} and Mr. Damm's rotors ^{subsequently.} were to be used commercially in a machine designed by Boris Hagelin, ^{1925 in} ~~in 1925. ⁶ ~~It was considered only a preliminary project.~~~~

Mr. Damm's death in 1927 provided Hagelin with the opportunity to purchase A. B. Cryptograph. The firm was reorganized as Aktiebolaget Crypto⁺teknⁱek. As technology advanced, Hagelin recognized that printing cipher machines were faster, ^{more accurate,} and more economical than ^{indicating} mechanism like the Enigma. ^{The} ~~result of this recognition was~~ ⁱⁿ the development of the ^{B-21. 7} ~~221.~~ (S)

In the following years revolutionary concepts ^{in cipher machine design} were achieved. The breakthrough came in 1934 with the completely new ^{line of} machines, designated as the C-series. (S) In 1934 the French requested that a pocket sized cipher machine be developed that would print cipher text in five letter groups and the plain text in normal word lengths at a rate of 25 letters per minute. To fill this request, ~~for cryptographic aid,~~ Hagelin developed the C-36. (S)

~~William F. Friedman~~

Friedman and Hagelin had been in close contact regarding development of the B211, but it was only in 1937 that Hagelin visited Friedman in Washington and demonstrated it to him and his colleagues. The discussions were mostly exploratory but the meeting was the start of a friendship between Friedman and Hagelin which lasted until Friedman's death. (10)

← out of chronological order

In 1935, Hagelin began corresponding with American cryptologic authorities regarding the C-36. During the course of communication, Friedman offered some suggestions to improve the C-36. Hagelin subsequently redesigned his C-36, incorporating Friedman's ideas and calling it the M-209. (10)

William F.

PUT FIRST

~~During this period a friendship between the two developed during this period and lasted until Friedman's death in 1969.~~

Early in 1940 when Germany invaded Norway, Hagelin decided that it would be in his best interest to come to the U.S. At the time hostilities broke out, Hagelin had been designing the finishing touches into the M-209. He had a couple of dismantled machines and a set of manufacturer's blueprints. In his determination that the machines be delivered to America, Hagelin, with his wife, Anne, embarked on a risky trip across Germany, carrying his machine and blueprints in a diplomatic courier bag. They reached New York on the last ship to leave Genoa, Italy. In the meantime, the U.S. Army insisted on having more machines for testing so Hagelin arranged to have fifty of the ciphering devices smuggled out of Sweden and into the U.S. (12)

Before the M-209 was accepted for use in the U.S. military, Friedman, Technical Director of the Signal Intelligence Service, turned in an unfavorable report on the machine, as he believed that although its cryptosecurity was theoretically quite good, it had a low degree of security if improperly used. However, he was overruled because, "... neither the Signal Intelligence Service nor the Signal Corps Laboratories at Ft. Monmouth had developed anything that was better than the Hagelin machine or even as good." (13)

The Army adopted the M-209 as its medium level cryptographic system. More than 140,000 were purchased and employed in military units from division to battalions. (14)

The M-209 was practically identical to the C-28³ (improved C-36) manufactured and sold on the open market by Hagelin in various parts of the world. ¹⁵ [In its operations in the COMINT World-AESA had knowledge of the extensive use of the C-38 by the foreign governments. (15).

NECESSARY?
IF NOT add FIRST
Sentence to ??
above

In 1944 Hagelin and his wife returned to Sweden since their operations were concentrated in Stockholm. Unfortunately for Hagelin, Swedish law enabled the government to appropriate inventions that it needed for national defense. Because of this, Hagelin moved his ^{research} operation to Zug, Switzerland in 1948. In 1959 Hagelin ^{moved the rest of his firm from there,} incorporated his ^{ing} firm as Crypto Akitengesellschaft, Crypto A. G. (16)

demolished problem again

In October 1946 Friedman visited Hagelin at his home in Zug, Switzerland and toured Hagelin's office where they talked over business matters. Their personal relationship was such that exchange of small gifts was commonplace. ~~X177~~ During Friedman's trip to Crypto A. G., Friedman examined old models of machines and while at the plant Friedman observed that there were good feelings between ~~Boris~~ ^{Hagelin} and his employees. On Friedman's departure he recalls that "I had almost tearful farewell with the Hagelins. They are such charming people and I hope they will come to Washington this spring as Boris and Anne promise." (17)

*observed
makes sense if
Crypto A.G. wasn't
named until 1959.*

*is an a
left out of
quote?*

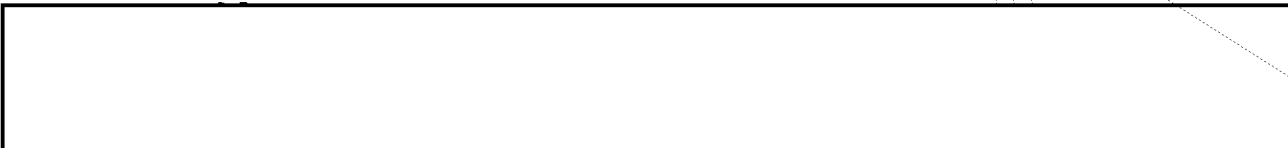
After ^{the} close of hostilities, ~~Mr.~~ Hagelin ~~researched~~ ^{made efforts to improve} improving the C-38 (or M-209) and to produce the new cipher machines for commercial exploitation. Through informal contact between ~~a member of (AFSA)~~ ^{the Armed Forces Security Agency} and Hagelin, some of Hagelin's new ideas for devices came to the attention of AFSA and were studied to ascertain their security. The results of such studies were not communicated to Hagelin.

*Spotted
in
first
time*

*probably
at AF*

~~Z. 111-15~~
In 1941 a modified M-209 incorporating a new keying mechanism was received and studied by AFSA. In addition to the modified M-209, ~~Crypto A. G.~~ ^{A. G. Cryptoteknik} had plans to produce several new cipher machines of considerable security employing the new keying mechanism. Hagelin filed patent applications in the U.S., Switzerland, France, and Italy. ~~The effect of~~ ^{since} the new and more complex cipher machines could have ~~the~~ ^a profound effect

6



became the subject of discussion within AFSA soon after U.S. receipt of the modified M-209.

Friedman, because of his long acquaintance with Hagelin,



informed the Director, AFSA. Friedman, on behalf of the Director, ~~AFSA~~ ^{Stuart} ~~Armed Forces Security Council~~ AFSA, presented the matter at an (AFSAC) meeting. AFSAC authorized the chairman to contact the Director, Central Intelligence Agency



After a number of meetings among Mr. Hagelin and his U.S. counsel, ^{Stuart} Mr. Hedden, CIA representatives and the Director, AFSA, Mr. Hedden submitted a draft agreement on behalf of his client, Mr. Hagelin. AFSAC decided that they could not endorse



However AFSAC indicated that they wouldn't object ^{to} to all

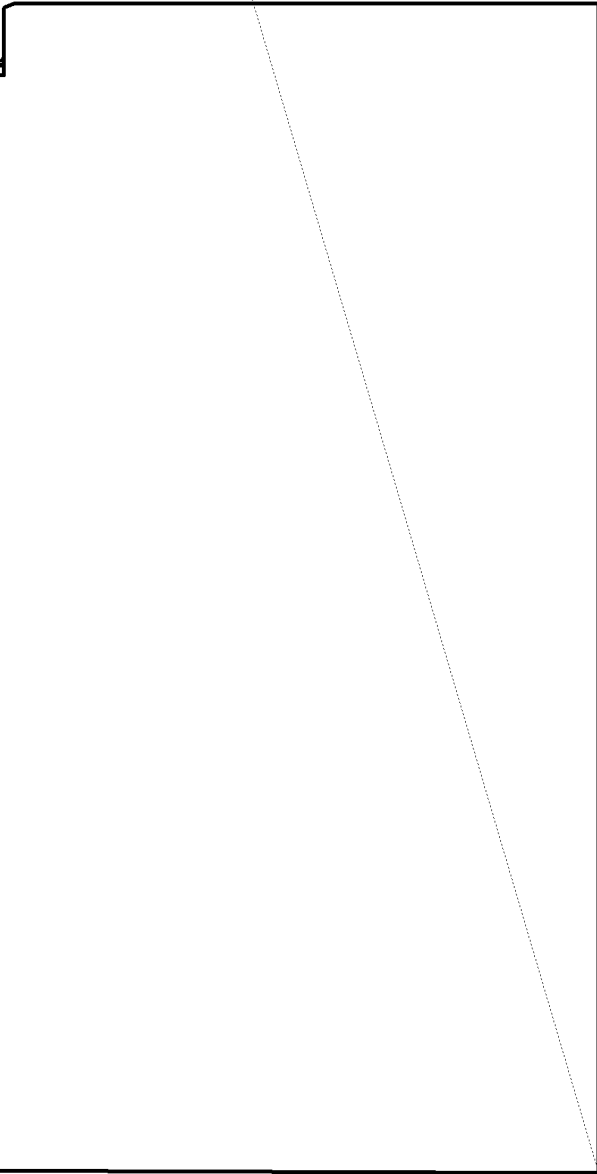
Very interesting
see enclosure C
"Negotiations with H. Felt"
Box 12

used for
Hagelin



being developed by Hagelin. *! Don't understand this sentence*

A revised draft Memorandum of Agreement was drawn up
by Mr. ^{Yostus E.} Becker of the CIA which, in essence,



*no discussion
of...*

and that, with regard to off-line

cryptographic machines, Hagelin had no competition. (1³)

8

[REDACTED]

France had requested that Hagelin refrain from selling his C-52 to Egypt. Hagelin gently complained to Friedman that, although the French imposed restrictions, he was glad to conform with their wishes because they gave him substantial orders;

[REDACTED]

offered then would hardly be adequate.

[REDACTED]

[REDACTED]

[REDACTED]

OGA

In late 1957 Friedman again visited Hagelin in Zurich and Hagelin insisted that Friedman be a houseguest. Hagelin



In January 1958, Friedman again visited Boris Hagelin and his family in Zurich. In their professional discussions, ^{Hagelin} ~~Boris~~ and Friedman discussed Hagelin's U.S. patent on the "Electric switching Device for Ciphering Apparatus." Friedman was surprised ~~at this~~ because this patent covered the re-entry principle in electric rotor machines, a principle which ~~was first~~ ^{surfaced} ~~thought~~ ^{in the U.S.} ~~of~~ ^{in 1940.} This concept had been documented and application ^{had been} ~~for patent~~ ^{filed for.} ~~]~~ All papers connected with the application had been placed in secrecy. The patent office should never have issued ^a ~~any~~ patent on the re-entry principle, a matter Friedman planned to investigate. ^{Hagelin} ~~Boris~~ was not informed of ^{the similar U.S.} ~~any of the patent matter or its irregularity.~~ ^{patent} ~~Hagelin told~~ ^{application.} Friedman that while the U.S. granted him the patent, the Japanese government declined to do so. (24)

when?

While in Switzerland, Friedman took advantage of the opportunity to visit Hagelin's plant and see new equipment models and developments. During the visit Friedman became aware of Hagelin's knowledge regarding ^{the} equipment radiation threat. (25)

Boris Hagelin, Jr

Friedman was worried because ~~(Bo)~~ was putting out instructional literature about cryptographic communications, insecure crypto-equipment and the faculty of good equipment. Boris Hagelin, who was having some problems with his willful son, told Friedman that U.S. authorities were in a better position to control this sort of thing than he was. (26)

Hagelin's

Not only was Friedman concerned about ~~Bo's~~ lack of discretion, he was also aware of new problems coming over the horizon. Hagelin had recently developed a cipher machine the size of a pack of cigarettes. Friedman saw another potential threat to U.S. SIGINT production. (27)

when?

During this trip Friedman found out quite by accident that Hagelin had plans to put out three versions of several Hagelin machines, ^{which were} either in production or ~~in~~ development. Hagelin himself never discussed ^{this} it with Friedman. Instead, it was mentioned to him by an employee of Mr. Hagelin. The three versions of the machines would be designated as "best," "second best," and "third best." The quality rating reflected the amount of security afforded by or built into the machine concerned. Radiation from equipments had ^{earlier} been discovered by Siemens and the information passed along to Hagelin. (28)

*more specific
what earlier?
or later?*

The T-55 cryptoprinter had three versions ready for sale in 1958. Version 1 was for the West, NATO, and countries friendly to

//

A.B. Cryptoteknik

them. It had the best features that ~~Crypto-A.E.~~ ^{was} could produce, ~~was~~ ^{was} fully protected against radiation, and had total usage flexibility. Version 2 was for friendly neutral countries like Finland. It was neither fully protected against radiation nor flexible. Version 3 was for countries of doubtful orientation or countries leaning toward the USSR. ³⁰ (28) what were characteristics?

In the summer of 1958, Hagelin confided in Friedman that he ^{was} ~~is~~ concerned about his son's relationship with Mr. Barlow (not further identified). The worry was that Barlow was influencing ^{Hagelin Jr.} ~~Bo~~ with regard to Hagelin's projects ^{and} business interests. Friedman requested both the Director and Deputy Director, NSA, to determine the nature of ^{Hagelin Sr's + Barlow's} ~~their~~ relationship. Friedman confided to Hagelin that

Footnote →



Friedman

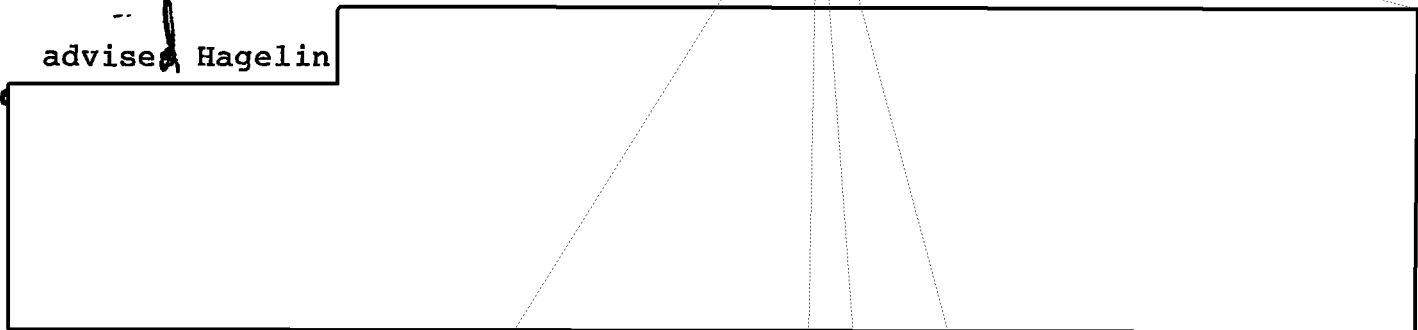
^{Hagelin Jr.} ~~he~~ added that he felt ~~Bo~~ had something against him and ^{that} future correspondence between Friedman and ^{Hagelin Sr.} ~~Boris~~ had to be purely personal greetings. Hagelin mentioned to Friedman that Barlow, during his last visit to Zug, did not show any interest in Hagelin's work. Boris felt that Barlow had been taken in by ^{Hagelin's} ~~Bo's~~ tales of woe.

In August 1958 Friedman informed Hagelin that the relationship between ^{Hagelin Jr.} ~~Bo~~ and Barlow ^{was} ~~are~~ social in nature. However, Friedman

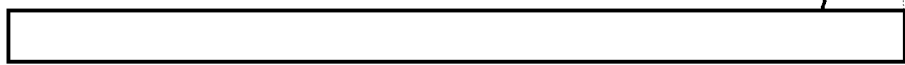
EO 3.3(h)(2)
PL 86-36/50 USC 3605

advised Hagelin

Restate



A few years prior to Friedman's death he confided in ^{Hagelin, SR.} Boris some details regarding his relationship with NSA. They shared many problems with each other, often personal ~~and private~~ in nature. As evidence of Friedman's regard for his old friend Boris ^{Hagelin,} Friedman sent to Hagelin a letter of introduction for [redacted] president of the [redacted] Friedman requested that Hagelin provide [redacted] with unclassified material to aid him in his research which eventually resulted



William F. Friedman and Boris Hagelin continued to correspond until Friedman's death in 1969.

1. Ronald W. Clark, ^{REF ID: A61628} ~~The Man Who~~ Broke Purple,
First published in Great Britain by Weidenfeld
and Nicolson, 1977, page 80

[REDACTED]

3 Advertising brochure for Crypto A.G., WFF collection
Box 12, D4.

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

[REDACTED]

[REDACTED]

6 Clark, The man who broke purple. p. 78

[REDACTED]

8 Advertising brochure for Crypto A.G. WFF collection
Box 12, D4

[REDACTED]

10 Clark, The Man who Broke Purple. pp 110-111

[REDACTED]

[REDACTED]

13 Clark, The man who Broke Purple. p: 112

[REDACTED]

15 negotiations with Hagelin, WFF Collection, Box 12, D4

17. WFF Diary, WFF collection, Box 1, D4

18. ~~WFF~~ Negotiations with Hagelin, WFF collection, Box 12, D4

19. Visit, WFF collection, Box 12, D4

20. ~~Sbid~~ ^{Sbid} (Visit Memo for DIRNSA (re visit to Stockholm))

21. Sbid

22. Sbid

23. ~~Sbid~~ ^{USIT} TRIP Report dtd 10 Jan 1958, WFF collection, Box 12, D4 p 6+9

24. Sbid p 26

25. Sbid p 1

26. Sbid p 8

27. Sbid p 26

28. Sbid p 27

29. Sbid p 14

30. Sbid p 30

31. Correspondence between Hagelin and Friedman, WFF collection, Box 12A, D4