

~~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

9
5

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~I. INTRODUCTION

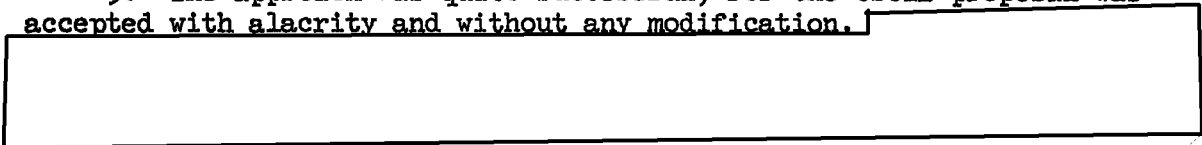
1. In accordance with Letter Orders 273 dated 27 January 1955, as modified by L.O. 273-A dated 4 February 1955, I left Washington via MATS at 1500 hours on 18 February 1955, arrived at Orly Field, Paris, at 1430 hours on 19 February, and at Zug, Switzerland, at 1830 the same day. I spent the next few 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.



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

~~TOP SECRET~~

~~TOP SECRET~~

II. STATUS OF NEW DEVELOPMENTS

1. Sales and Prospects of Sales of C-Line of Machines. -- The following information under this heading was given mostly by Hagelin Jr., who either had the data in memory or had quick access to the records pertaining thereto:

a. The present manufacturing capacity of the Hagelin plant in Stockholm for the manufacture of the C-line of machines (C-52, CX-52, etc.) is 60 to 80 machines per month; the goal is to increase this to 100 per month as soon as practicable after the Stockholm plant is closed down and the new plant in Zug is well established (see para lb below). No manufacturing quotas were mentioned with regard to other machines; the latter are still in the development, prototype, or pre-production stage.

b. Decision has been made to close down the plant in Stockholm and to move such of its manufacturing tools and equipment as is deemed advisable or necessary to Zug, where two new buildings are to be prepared for production of the new lines of machines. One of these buildings is an existing structure which is to be modified to suit the need for additional space for operations but its top floor is to be made into an apartment for the chief engineer, Mr. Sture Nyberg, presently in Stockholm but scheduled to move to Zug as soon as the apartment is completed. The other building is to be newly constructed and the excavation therefor has been completed; its top floor is to be an apartment for Boris Hagelin, Junior and his family. The three buildings (the two above-mentioned, plus the present research and development building) are adjacent to the home of Boris Hagelin, Senior, so that the new plant comprising Crypto A.G. will be a compact, homogeneous set of units. I was told by Hagelin Junior that his father expects to retire from active direction of Crypto A.G. in two years (at age 65), although undoubtedly he will continue to have a voice or hand in direction thereafter. From one comment made by Hagelin Senior, I gathered the unmistakable impression that he plans to let Hagelin Junior take over the Crypto business and direct its affairs when he himself retires.

c.(1) The plant in Stockholm, besides being now engaged in manufacturing of new C-52 and CX-52 machines, is also to fill an order for 500 to 1,000 machines of the old C-446 type. (See paragraph f(14) below.) In order to execute this order some or most of the tools for making the C-446 will have to be rehabilitated or else replaced with new ones. I asked Hagelin Senior if he needed any financial help in this regard; his answer was in the negative, since, as he said, he

~~TOP SECRET~~

estimated the cost of rehabilitating the old tools or making new ones to be only about \$10,000. However, he indicated that he might like to have some help in building up his new plant in Zug for without it he will have to sell some of his liquid capital assets (stocks and bonds). I made no comment and the matter was not referred to again. I wish to point out, however, that the rehabilitation of the C-446 tools offers certain potential advantages to UKUSA; for once these tools have been rehabilitated, Hagelin will be able (as he himself mentioned to me) to make more C-446's than are needed by the government for which he is making this old model. In other words he was hinting to me that this rehabilitation would make it possible for him to supply certain customers with a model almost like the M-209. This model is, of course, easier to solve than the new models and [REDACTED]

OGA

(2) The present space occupied by the Hagelin plant in Stockholm will be turned over to the Johansen Gauge Company, together with all of the C-446 tools, jigs, and dies; these are to be held by Johansen on loan until the order for the 500 to 1,000 C-446's has been completed. These tools, jigs, and dies, together with certain machinery will then be shipped to Zug. The Johansen firm is to take over and employ all or most of the Hagelin workers in Stockholm, except Chief Engineer Nyberg, mentioned above.

d. (1) It may be well at this point to set forth specifically the different models or machines which are comprised in the C-line, using designators which the Hagelins and I agreed would be suitable. The C-line machines are readily classifiable (according to Hagelin Senior) into two main classes:

(a) Class 1 -- Where all keywheels advance the same number of steps. In the case of the M-209, of the C-446, and of a certain version of the C-52, the advance is one step. [REDACTED]

In this class the machines are not to be equipped for operation with a one-time tape (OTT).

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

~~TOP SECRET~~

(b) Class 2 -- Where the stepping is irregular and where OTT readers are provided, as well as equipment for producing the tapes.

(2) Based upon the foregoing categorization, in Class 2 there are the following models:

(a) CX-52a: The model with Standard A slide bars (for the cage), which produce irregular or varying angular displacements of the key wheels, each wheel advancing 0, 1, 2, 3, 4, or 5 steps per operation;

(b) CX-52b: The model with Standard B slide bars (for the cage), which produce regular or fixed angular displacements of the key wheels, all wheels advancing the same number of steps but the number may be any one from 1 to 32;

(c) CX-52c: The model which is compatible with the old types of C machines, the M-209, the C-446, or a certain version of the C-52 machine;

(d) CX-52ak: A CX-52a with the (Huettenhain) "komplimentary" feature incorporated therein;

(e) CX-52bk (or CX-52ck): These are likewise the same as CX-52b and CX-52c but with the complimentary feature incorporated therein;

(f) CX-52/10 and CX-52/30: These are CX-52's for 10-character ciphering (digits for enciphering numerical code groups) or for 30-character ciphering (30-element alphabet). These machines can be of the a, b, or c type, and can also be provided with the complimentary feature. (Example: CX-52ak/10)

(3) In Class 1 there are the following models:

(a) C-52: The model which is compatible with M-209 and C-446, but also can be made to function with interchangeable key wheels and with key wheels of larger numbers of elements than M-209 or C-446, so that a set of key wheels can comprise more than the 6 wheels now incorporated in the M-209 or C-446. Also the C-52 can be provided with a larger number of slide bars than has the M-209 or C-446.

(b) I presume that there can be a C-52/10 or C-52/30 but these were not mentioned; and at the moment I do not recall asking whether there could be a C-52a, or C-52b, or C-52c, or C-52ak, etc. I could no doubt ascertain this point easily enough by asking either of the Hagelins.

~~TOP SECRET~~~~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~~

~~TOP SECRET~~~~TOP SECRET~~

C-52 to a C-52Y and that we could do it with the one he is sending us from Stockholm (at my request) by air; all we would need would be the special instructions for the slide bar and lug arrangements and he is to provide these instructions soon.

(4) A few minutes later Hagelin Senior read me a paragraph from a recent letter from the Italian defense department, in which it was stated that they were withholding an order for new Hagelin machines until more becomes known about what had been decided with regard to the various levels of NATO communications. Hagelin Senior wanted to know whether I thought there was a possibility that a Hagelin machine might be adopted for 3rd level NATO communications. I indicated that this was certainly conceivable and that that was why I was so interested in the proposed shift from CX-52 to C-52Y manufacturing, for I pointed out to him that NATO COMSEC authorities would have to be sure of the security of the new model and that detailed studies would certainly have to be made of the C-52Y before it could be given serious consideration for possible NATO usage. It was then that Hagelin Senior said that he would hold up on the C-52Y if we wanted him to do so.

f. Following is information regarding sales of machines of the C-line:

(1) Egypt -- now negotiating for 50 C-52 machines. They also want 10 BC-52 machines. They are waiting until an agreement can be reached as to prices. No final decision has yet been reached, either, as to whether their machines are to have Roman or Arabic characters. I asked Hagelin Senior whether there had been any trouble with the Egyptians because they weren't being given the CX model. "Well, the only thing they can have now is the C-52. We just stopped talking about the CX; we talked only about the C-52 and they were satisfied."

(2) Jordan -- has bought (about) 30 machines; 10 are C-52's and 20 are BC-52's. Hagelin is going to make delivery soon. He said: "I have a very good agent there. These machines are for the Arab League and the Foreign Office. It is the British who are behind this purchase -- it's they who are paying. The Jordan Chief Signal Officer is a Britisher."

(3) Iran -- The Hagelins have no agent in that country. There seems to be no interest there in cryptomachines, according to Hagelin Senior.

(4) Iraq -- is negotiating for an order of about 50 to 200 C-52's with Arabic characters. "They have a more than lukewarm interest."

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

(5) Syria -- has recently purchased 50 C-36(sic) machines. I asked Hagelin Senior where in the world he found so many of that old model; "We had some down in the basement in Stockholm."

(6) Saudi Arabia -- only some correspondence exchanged recently. Hagelin has no agent nearby.

(7) India -- was shown only the C-52 model. The Hagelins felt quite certain that the Indians will order some of these machines, and they are also definitely interested in the BC-52. [Hagelin Junior on his recent trip, it will be recalled, did not demonstrate the CX-52 to any of the Arab countries, nor to India.] "The Indian Army is interested in these machines, too. They want to have a lot of BC-52's for test purposes. Don't you think that queer?" I said that it seemed a bit unusual to ask for a lot of machines merely for testing.

(8) Pakistan -- is waiting for a model of the C-52 for Hindustani (which has 29 or 30 characters).

(9) Belgium -- The Armed Forces have ordered more than 200 CX-52's and about 160 have already been delivered. These are CX-52a's with variable typewheels. The Belgian Foreign Office have C-446 machines and will stick to these but have bought 100 variable typewheels.

(10) France -- "The French have had the CX-52 two years already, for study." The Foreign Office has placed an order for about 100 machines; 80 CX-52a, 20 CX-52a/10. [The Armed Forces are much more interested in the HX machine," Hagelin said. I will have more to say about France later in this report.]

(11) Portugal -- bought five CX-52a's.

(12) Italy -- no action yet. "They are 'bellyaching' about 'what will NATO do.'" Hagelin Senior stated that endorsement of the CX-52 would serve as a real stimulus to their placing an order.

(13) Greece and Turkey -- have been given literature and are interested. Hagelin Junior is supposed to have gone there long ago for a selling trip, but has postponed the journey -- no date mentioned.

(14) Holland -- The situation with regard to the Dutch is interesting in view of the Petersen Case. They are sticking to the C-446 in the main; this is certainly true as regards the Foreign Office.

~~TOP SECRET~~

~~TOP SECRET~~

Referring to the renewed manufacture of the old C-446 type of machine (mentioned in paragraph c(1) above), these are for the Dutch Government. Most of these machines are for the Dutch Foreign Office but a good many are also intended for the Dutch Army. According to Hagelin Senior, the Dutch Foreign Office finds the C-446 quite satisfactory because, as they say, (a) they are well organized now for using that model and (b) the new models are much more expensive than the old ones. (Hagelin Senior commented that Dutch thrift resents having to pay more than they think warranted.) However, though the Dutch Foreign Office likes the C-446, it wants a certain number of their new C-446's to be provided with means for using one time-tape control of the stepping mechanism instead of pin-wheel control. The development of the tape-control mechanism has given Hagelin some trouble but the problem was recently solved. Hagelin Senior stated that the Dutch Army is much interested in the new CX-52 model and wants to obtain some machines of that type as well as a number of BCX-52's.

(15) United Kingdom -- "The British bought two CX-52's. They paid for them, moreover, in Free Swiss Francs and they didn't relish this."

(16) Germany and Austria -- Dr. Hell (who by contract supplies the West Germans and West Austrian market for C-line machines) has assembled ten CX-52's for the Bonn Government. These are CX-52bk type, -- "the only model which is approved by Huettenhain." [The personal relations between Hell and Hagelin are still very cordial and their contractual relations are the same as related in my previous report.]

(17) Sweden -- is going to replace all its C-446 machines with CX-52's in a long-term replacement program, with a more or less fixed amount of money available each year for this purpose. I asked Hagelin Junior what the Swedish Government's reaction had been to the decision to move the Stockholm plant to Zug. His reply: "They don't like it, of course, but have become reconciled to the idea. What else could they do?"

(18) Spain -- has shown a great interest in C-52 but has placed no order as yet. They are also interested in other new Hagelin products.

(19) Eire -- has recently placed an order for two CX-52's. These are soon to be delivered.

(20) Indonesia -- "We had quite a messy business correspondence, back and forth, but now they have finally decided to place an order for

~~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: Ed

3.3(h)(2)

86-36/50 USC 3605

(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) Argentina -- 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.

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

(28) Paraguay -- no interest.

(29) Uruguay -- bought five CX-52's and two BCX-52's.
 "That's their first experience with cryptomachines."

(30) Colombia -- has ordered about 100 CX-52's and about
 40 BCX-52's.

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

2. a. In discussing with both Hagelins the matter of new developments in crypto-apparatus and their sales promotion, they both stated that they are sometimes confronted with a considerable amount of sales resistance which arises from excessive nationalism and which makes it difficult for a country to accept machines invented or manufactured in some country other than its own. France, for instance, wanted to use only such machines as were invented or made in France. [This statement makes me suspect that the French have told Hagelin about the machines furnished them recently by the U.S. and the U.K.; perhaps this feeling on the part of the French has a bearing upon their dilatory conduct in regard to putting these machines into usage.]

b. I said to Hagelin Senior that Boris Junior had told me that his father had again been to Paris recently and that I imagined it was in connection with the modification to the B-211. When he nodded affirmatively I said that I was glad to learn that he was trying to help the French, for they were our allies in NATO. I asked him if he could give any reason for the recently heightened interest in crypto matters on the part of France. He said he thought that increased interest was a result of Viala's coming into the picture in the Foreign Office. Viala* wanted to replace the

*Hagelin said that there is another, unrelated Viala in the crypto business for the French Department of the Interior.

~~TOP SECRET~~

~~TOP SECRET~~

old-fashioned methods and Foreign Office codebooks with more up-to-date things. Viala is a forceful character, he said. But he added that Viala, of course confines his activities in this regard to the Foreign Office. He went on to say that the "Commission de Chiffre" under President Ollier is now very active. Captain Mueller, a member of the Commission, representing the Presidence de Conseillers, is also very active. Ollier is a man 40 to 45 years of age, rather cold but Hagelin sized him up as being extremely intelligent and a very strong character. Hagelin said he could tell me about some very important French plans for improvement in crypto affairs. For one thing, for example, the French Government is going to establish a plant in Paris but as a private enterprise. "There is plenty of money behind the people who are prepared to do that. The Government will buy the tools, since they want to be sure to have all the tools necessary for manufacturing their machines, but the plant itself will be under private ownership. This ownership will probably be that of a subsidiary of an already well-established firm called the Société Electronique Automatisation (SEA), which, though a relatively new firm, is already a very important concern making electronic computers. Its president is M. Raymond, a young man but supposed to be first in France in technical know-how as regards such machines. The people behind SEA have plenty of money -- they are considerably higher up in Government affairs than people like Colonel Arnaud, who is constantly being needled by Ollier to get busy on this crypto manufacturing business. The plant will start with making HX (electric rotor) machines; possibly also CX machines."

c. (1) The B-211 modification, designed and developed by the Hagelins, has turned out to be quite successful, according to Hagelin Senior. What I saw of this development (in Paris last September) was merely a rough design; they had worked it out in practice so that it can easily be added to the existing B-211; his agent in Paris (M. Rene de Chauny) will probably do the work on the machines when the latter are sent to him in batches for servicing. The Hagelin firm had an order for 250 B-211 modification kits for the French Army and 200 will probably be ordered by the French Air Force. "Captain Mueller told me that with this improvement the modified B-211 will be more secure than the original British TYPEx" (meaning, Hagelin said, the "type with the simple reflector -- not the one with the straight-through circuiting and reversing switch"). Hagelin commented that the French had something on their B-211's which was not put on by him and hence he didn't know what it was. The parts for the modification kit will be made in Zug, either by Crypto A.G. itself or by a sub-contractor in Zug.

(2) I asked Hagelin Senior whether this modification kit for the B-211 would be available to other owners of that machine. "There

~~TOP SECRET~~~~TOP SECRET~~

aren't any others now." "Oh, but we have some," I said, to which he made the laconic comment: "Yes, two." I said: "Yes, and you will recall also that I have one personally, one you presented to me for my collection -- the one formerly owned by Ivor Krueger." Then he went on to say that he would do the conversion in Zug on our two or three machines at such time as would be convenient.

3. a. Relations with Siemens and Halske are now formalized in a signed contract. Siemens agreed to stay out of the cryptomachine manufacturing business and confine itself to the teleprinter manufacturing business; Hagelin agreed to stay out of the teleprinter manufacturing business and confine himself to the cryptomachine manufacturing business. In case in the future Siemens wished to go into the cryptomachine manufacturing business they must give Hagelin notice thereof and for at least one and a half years after giving such notice they must stay out of such manufacturing.

b. Hagelin Junior showed me the last page of the contract with Siemens, in which the marketable areas for telecipherring machines were divided between Siemens and Hagelin as follows:

- | | | | |
|---|---------|---|--|
| (1) Siemens alone: | | (2) Crypto A.G. alone: | |
| West Germany }
West Austria }
Jugoslavia }
Portugal }
Ireland } | Europe | France }
Italy }
Switzerland }
Sweden }
Norway }
Benelux } | |
| All except }
Brazil, USA, }
and Canada } | America | Brazil | |
| All except Egypt | Africa | Egypt | |
| All except India, }
Indonesia, China } | Asia | India | |
| All Australia | | | |
| (3) Siemens and Crypto A.G. together: | | | |
| Denmark }
Greece }
Spain } | Europe | | |

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

Siemens and Crypto A.G. together: (Cont'd)

Indonesia	Asia
None	America or Africa

(4) Areas not yet assigned or clearly agreed:

Finland
 Russia and all satellites
 East Germany
 China
 USA and Canada

4. Rather casually, I asked Hagelin Senior, but in the presence of Hagelin Junior, why, if they were moving the Stockholm plant to Zug, they hadn't considered moving the whole business to the U.S. He replied: "You'll have to ask Bo about that." I said, "Why Bo?" Boris Junior answered somewhat quietly: "I suppose he means for me to carry on the business. What would be the advantages of moving the business to the U.S.?" I said: "Well, I thought you didn't like Switzerland at all, and the same goes for Edith, doesn't it?" His reply: "We're both getting better adjusted to living in Switzerland. And then soon, when the Nybergs have settled down among us, we'll have some agreeable company." Hagelin Senior: "I suppose the U.S. could and would bind me with restrictions so I couldn't be free to export where I please." I said that I supposed that certain things could be done along that line -- there were, of course, restrictions on sending instruments of war or material for war to countries behind the Iron Curtain. But I added that I didn't think the U.S. would be tough or have a very rough policy. I did not pursue this subject any further, nor did they. Later on, Hagelin Junior's wife (Edith) confirmed that she was getting better adjusted: "It takes a couple of years, you know. I was so upset last year that my doctor sent me to a psychiatrist but after the one and only one visit I made up my mind I didn't need such help and would help myself out of the spell." [She did look much better than when I saw her last September.]

5. a. The new base for the BC-line (electrically operated keyboard machines) was shown me. It looked extremely simple and compact. Any C-52 or CX-52 need merely be placed inside the frame and fastened down by two screws, thus becoming a keyboard machine. To adapt the base to take a C-446 or an M-209 requires some modification but Hagelin felt that this could be done though he questioned the practicability of doing it, because the shaft on which the keywheel assembly and the print wheel

~~TOP SECRET~~

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

is borne in these models is too short. This new BC base would facilitate operation by OTT and the sensing part of the mechanism for operating a C-52 or a CX-52 (or, eventually and possibly a C-446 or M-209) by means of OTT is now worked out so that the same mechanism will do for all.

b. This new base for the BC-line will cost about \$800. When I commented that I thought that a pretty stiff price for what was shown me, Hagelin Senior replied that he usually charged what the traffic would bear but at that price the cost of the base plus the cost of the C or CX machine itself, the total cost will still be less than that of the old BC-446, which was 8,000 Swedish Kronor, whereas the cost of the new base plus the C or CX comes to about 6,000 Kronor. On a big order for BC machines he would, of course, make a price adjustment.

c. The B bases are now being made in Stockholm (about 25). Zug will begin making them in about 10 months, according to the Hagelins.



6. One electronic OTT generator, called the ZG machine (Zufalls generator = Random generator), was designed and built in the Zug research and development plant in five months by Hagelin engineer Stürzinger. It was just recently turned over to the French Foreign Office for study and assessment by the Commission de Chiffre. No tests for randomness were made by Hagelin. This model uses a Creed perforator and produces one original and one copy. It is not equipped with marking apparatus which, Hagelin Senior said, "is the heart of the job. The French are going to work that out." He expects an order for several more of these OTT generators from the French. He also is making 3 or 4 for Denmark, Danish Navy Captain Weilbach being much interested in this machine. Belgium has also placed an order for one machine.

7. a. Crypto A.G. (Zug) has made parts for a first series of ten OTP producing machines (CBI-series) and one machine was assembled and operated for me during my stay in Zug. The machine is astonishingly small in size (about 1 cu. ft.) but weighs (I estimate) about 50-60 lbs. It prints in a single operation a line of 8 groups of 5-letters but can be made to print 10 such groups per line. Present operating speed: 7 to 8 lines per minute. It can also produce similar length lines and groups of

~~TOP SECRET~~

~~TOP SECRET~~

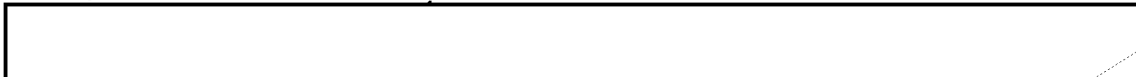
digits. I have brought back with me a sample of each (letter groups and figure groups) for preliminary testing. The machine easily makes one carbon copy and I imagine that it could make two carbon copies, though Hagelin Junior was dubious thereof.

b. Of the 10 machines constituting this first series, 7 are already sold, to countries as follows:

U. S.	}	1 each
Italy		
Portugal		
Belgium		
France		3

Crypto A.G. hasn't tried to sell any more of these as yet. Hagelin Junior mentioned that in his talks in India he learned that the Indians are now using IBM for making their OTP's but became much interested in the new Hagelin OTP machine. A retired general officer (Indian) came recently to Zug for a look-see.* There is a possibility that U.S. will buy one or two more. The 1st machine for the U.S. will be ready for delivery in 1 - 2 months.

c. Hagelin Senior said that Dr. Huettenhain had tested the end product of the prototype CBI machine some months ago and stated that the letter Z was unbalanced compared to the rest of the letters. Hagelin Senior said this had been corrected to a large degree but in future models they were not going to combine letter-group production with figure-group production in the same machine; two separate machines would be offered and they would be faster, simpler, and produce a more random end result. Hagelin Junior told me that they weren't going to make any profit on their first 10 machines and I imagine they would be glad to sell them all. Hagelin Senior asked me if U.S. could use more than one. I said we'd want to test the end product of our first one as soon as possible and that it might be that we would have use for several if they were really good. Hagelin Senior then reminded me (which reminder I didn't need) that General Canine had once indicated we would buy at least a couple. These machines are expensive (about \$5,000) but, of course, practically all the parts are hand-made. However, small countries would not need more than one or two such machines--



*Hagelin Junior said the Indian Signal Corps is also interested in the Hagelin teleciphering machines.

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

8. a. The status of the HX development was discussed. Some progress has been made in regard to the type of rotors that will be used; Hagelin Junior talked about their using printed circuits, a matter being investigated for them by an English firm the name of which was not mentioned nor did I ask for it. The new machine is now definitely to have 10 rotors, as mentioned in my last report, and he showed me a prototype rotor with 32 contacts. The rotor was about $1\frac{1}{2}$ inches in diameter, the contacts of silver. I asked Hagelin Senior whether the HX-54 was to be a 26-character machine and, if so, what he proposed to do about the 6 extra characters. (This question was also asked in the course of my previous visit.) He told me that these 6 extras would be re-entered from the output side into the input side of the maze. [I wondered whether I should ask him if he had put in for patent coverage on this idea but decided not to ask. The U.S. has one in secret status in the U.S. Patent Office.]

b. Two prototypes of the HX-55 will be ready before June 1955. There will be three crypto-components for these, that is, there will be one spare crypto-component, for test purposes.

c. I told Hagelin Junior that the sooner they could get us an HX-55 the sooner could an answer be given as to the security of the machine.

d. The Hagelins demonstrated a bench model of the slide bar and rotor drive mechanism for the HX machine, using the C-52Y principle. This component was very quiet in operation and quite rapid. However, the unit used was the same 5-rotor assembly that was in the HX-54 I saw on my visit last September, not the new proposed 10-rotor assembly.

9. a. Hagelin Senior has definitely given up the idea of having "a single package machine," that is, one that can be used both for on-line teleciphering as well as for off-line literal operation in a single apparatus made up of several components. He gave up the idea "because (1) it would take much longer to develop than he could afford at this juncture of his research and development; and (2) the Siemens people didn't like the idea and I don't want to buck them." Hence, he is going to have one off-line literal machine which might be the HX-55 or even HX-56; and a separate on-line teleciphering machine.

b. The first model of his on-line machine (TL-55 or 56) will employ merely the 5-unit code baud addition by the Vernam principle, controlled by OTT. The second model (TC-55) will also use baud addition.

~~TOP SECRET~~

~~TOP SECRET~~

but this will be controlled by the same cryptomechanism and principle as that to be incorporated in the C-52Y; the third model, still an on-line teleciphering machine (TCX-55) will use the cryptoprinciples of the CX-52 machine; and finally, a fourth model (TH-55 or 56) will use the HX cryptoprinciple (10 electrical rotors, with 5 to 32 and 32 to 5 translators). All of the latter three models of machines will also be operable by means of OTT. Hagelin is trying to produce prototypes of the new teleciphering machines as soon as possible, but so far they have only sketches, not even good drawings. Still they hope to have prototypes this year.

c. Hagelin Senior told me that he was going to try to eliminate rotors from the TH-56 and use relays instead. He thought that with about 400 relays he could accomplish what the rotors do. He did not mention the word "electronic" in this connection, nor did I, of course.

d. No more of the present TC-52's or TL-52's will be produced; of the former a total of 20 was to be made and these have been completed; of the latter, a total of 50 was to be made but only a few have been completed. These machines are for the French Foreign Office, Army, and Navy -- no Air Force, because they are tied up with SAGEM which has recently improved its model but still uses the cryptoprinciples employed by Hagelin in the prototype he built for SAGEM. (The U.S. has placed an order for one TC-52, and, I think, for one TL-52.)

e. Hagelin Senior stated that Egypt and India are interested in having teleciphering machines controlled by the C-52 principle, and these would be provided with but one tape reader (not two, so that the machine could not be operated by OTT.) He asked me if I thought it would be O.K. for him to provide them with machines of this type. I told him I thought this might be satisfactory.

10. a. The new pocket cipher device (CD) appears to be well under way and the Hagelins are enthusiastic about it. This device will use six notched disks made of plastic (the customer breaks off pieces on the periphery to make the notches; this will make the disks equivalent to the pin wheels of the C-line machines. In fact, the CD will have the C-type cryptoprinciple, but it can also be given the CX-52 cryptoprinciple. Since the CD will not have lugs on slide bars, there can be no "overlapping," but the CD could easily have seven or eight disks instead of only six; or it could even be operated by OTT. One keying mechanism has already been built at Stockholm; it is the size of the transistorized radio set I bought for him in the U.S. I gathered that the CD will produce a printed record ("the print unit is really very simple"), but my

~~TOP SECRET~~~~TOP SECRET~~

notes also say that "the CD will have C-type motion controlling two concentric alphabet rings."

b. The history of this development may be of interest. Part of it was related to me privately by Hagelin Junior with the request I say nothing about it to his father. According to Hagelin Junior, many of their customers for several years in the past have importuned the Hagelin firm with the request that they be provided with a pocket-size cryptodevice, and he (Hagelin Junior) had in 1951 or thereabouts proposed a mechanism for such a device -- the same or nearly the same as that incorporated in the present CD prototype. But Hagelin Senior was not interested in such a project and rejected Hagelin Junior's ideas -- until an ex-Hagelin employee, one VIGO LINDSTEIN, came out recently with a pocket-size device. /Note: This is the TRANSVERTEX device the Swedish Government turned over to the Norwegian Government, which turned it over to NATO COMSEC authorities; it is now being given security studies by UKUSA. How the Hagelins learned about the Lindstein device is not known to me; it is held in a secret status by the Swedish Government and has been from the beginning handled as SECRET in NATO and UKUSA, so far as I am aware./ When Hagelin Senior learned of the Lindstein device, he then became much interested in such a project and somehow or other considered the ideas originally proposed by Hagelin Junior as his own. When Hagelin Junior learned that Hagelin Senior had decided definitely to turn over the Sundsör brick manufacturing works to his other son (Gunnar), Hagelin Junior said to his father that in view of what he was doing for Gunnar he should at least turn over what royalties there would be on the new CD to him (Junior); whereupon his father went into a rage, apparently claiming all credit for the CD himself. "It's not nice of me to say this much about the matter, but that's the way it was."

c. I asked Hagelin Senior what usages he could foresee for the CD. He felt that secret agents, small military units, or patrols could find good use for it.

11. a. In connection with the 5 to 32 and 32 to 5 translator principle to be used in the proposed fourth model of the on-line telecipherring machine (THX-55 or 56), a principle which incidentally the U.S. uses in one of its own new developments, Hagelin Senior stated that he was afraid he was going to have some difficulties with the Lorenz people in Germany. That firm has a German patent (elsewhere, too, I think) on the means for accomplishing or using that principle, application for patent having been entered in 1943 and just recently granted (January 1955). Hagelin Senior showed me the German patent and he is to send me the numbers of the whole series which Lorenz has in Germany and in other countries on this translator

~~TOP SECRET~~

~~TOP SECRET~~

mechanism or on other items of interest. [Naturally, I did not say anything to Hagelin about our use of the translator principle but I am beginning to wonder whether the U.S. may not have similar trouble with Lorenz.]

b. One Lorenz patent, also entered in application form in 1943 and granted in 1955 was, however, killed when Hagelin showed prior use of the item. I am to get that patent, too.

12. a. With reference to what the Bonn Government may be doing now with the Huettenhain crowd, Hagelin Senior said he was told that for Bonn there would be "a small machine made by Dr. Heil. That would, of course, be our own machine, the CX-52bk." But there would also be "a large machine, made not by us nor by Siemens, but probably, I think, by Telefon und Normalzeit (T & N Co.)." Hagelin said that he did not know any details, for those were classified. I asked: "Couldn't it be Lorenz rather than T & N?" "I don't really know," he replied, "It could well be. I suppose Lorenz did some work on cryptomachines for the Germans during the war, just as did the firm WANDERER in what is now East Germany. They stole my cipher pinwheel and slide-bar-with-lugs ideas and constructed a machine in 1944, you know." [The SG-41; Hagelin has one of these in his office.]

b. In a later talk with Hagelin Junior he asked me whether, with West Germany now or soon to be free, they will establish laws, such as in Sweden, prohibiting exporting certain kinds of equipment to certain countries. I told him I supposed they might well do something along those lines. He asked me to send him, if possible, what information there was and which could be made available with reference to such prohibitions. It seems that the Hagelins are worried about the competition they might get in future from such firms as T & N, or the one that made Enigmas; if West Germany would place a ban on exporting cipher machines the Hagelins would feel much more secure against the possibility that such firms "would peddle their machines abroad and give us serious competition." I said I'd see what literature or documents were available to send them for information on exporting bans.

~~TOP SECRET~~~~TOP SECRET~~III. THE APPROACH TO HAGELIN AS AUTHORIZEDIN USCIB: 29.14/29 OF27 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,

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 continuing to do for various members of his family. He hoped that everything would turn out well with regard to his son-in-law Conradi and his retention on active duty status in the USAF as a result of our intervention -- "the young man keeps assuring me that he is working like hell." He and his wife appreciated very much what we had done for her cousin (Miss Barth) in making a place for her in our organization.

USCIB. I told him that he need not give his answer there and then but could take his time to think it over, if he wished.

OGA

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

~~TOP SECRET~~

e. Hagelin Senior thanked me but said he did not need time to think the matter over; he was prepared to

f. I thanked Hagelin for his ready acceptance of our proposal and said

that if he wanted me to do so I could perhaps give a precis of the proposal to him or to Boris Junior in writing. He thanked me for this gesture but said he'd prefer not to have anything like that in writing. However, he would appreciate it if I would convey the proposal orally to Boris Junior myself. This I did the following day but by that time Hagelin Senior already had a chance to tell his son very briefly the substance of the proposal and of his own acceptance. Hagelin Junior also was ready with his assent. [I do not think that if he had withheld his assent it would have made any difference in the situation or to Hagelin Senior, for the latter had said, when he asked me to talk with Boris Junior about the proposal that even though his son was young, enthusiastic and wanted to make money, he "would be kept in line."]

I said I was sorry and I hoped they would not be embarrassed if they themselves, the producers of the machines, were not also authorized to be recipients of such instructions.

i. Nothing was said on either side as to the term of the "understanding," that is, how long it was to continue in effect.

j. The Hagelins wanted me to identify by name the authorities; this, they said, would be of great interest and help to them in their business. I told them I could not do so now; I could only say



OGA

TOP SECRET

[redacted] I asked that they be patient in this regard and that it would perhaps be possible to give them more information later. In any case, it was not they who were to ask for any endorsement, but the NATO customer who had to take that action, addressing their inquiry themselves to the NATO COMSEC authorities; they would know where or whom to address their inquiry.

k. Hagelin Junior said (but not in the presence of his father) that up to this time he did not ask [redacted]

[redacted]

14. In my last report of a visit to Zug, I mentioned Hagelin Junior's urgent desire to acquire a TYPEX machine which he could turn over to Mr. Rossby (mentioned above in paragraph 1f(21)), who was anxious to obtain one. Hagelin Junior brought this subject up again, said that Rossby was still very anxious to get his hands on a TYPEX, and that when he (Hagelin Junior) learned on his trip to India that the Indians had some TYPEX machines he tried to get one from them but was not successful. He went on to say that Rossby somehow or other got hold of a copy of the instructions for operating the machine but this, Rossby said, was not enough for his needs. Hagelin Junior said that he didn't necessarily have to have a machine in perfect operating condition -- one that worked only haltingly would do. He was quite in earnest about this and I think that if he could acquire a machine through U.S. or UKUSA action such a gesture would certainly cement good relations with Hagelin Junior, for, he said, "I am sure I could get for myself a new automobile out of such a deal."

28 March 1955

William F. Friedman

OGA

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



**NATIONAL
SECURITY
ARCHIVE**

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu