# Crypto AG : ’Le coup du siècle’

HAGELIN-CRYPTOS

CRYPTO AG

# Boris Hagelin

- Née en 1892 en Azerbaïdjan
- Fils d’un industrielle Suédois dans le pétrole qui supervise des opérations avec la Famille Nobel
- Il fait des études d’Ingénieur en Suède
- Rejoins AG Cryptograph en 1922 pour mettre au point la B-21
- 1932 : AG Cryptograph > AG Cryptoteknik


B-21

Enigma

- Au début de la Guerre Hagelin se réfugie aux États-Unis prenant avec  lui un prototype du futur modèle M-209
- Il fera par la même occasion la rencontre de William F. Friedman qui est un cryptologue de renommé mondiale et se lie d’amitié avec lui

Boris et sa femme arrivant à New York

William F. Friedman

M-209

# Le début de Crypto AG

- Hagelin s’installe en Suisse et commence de nouveaux prototypes
- 1952 > Crypto AG
- La CIA s’intéresse à Hagelin et font appelle a Friedman pour passer un accord qui sera nommé « The gentleman’s agreement »
- Les États-Unis rentre dans ce qu’on appelle une opération de déni

# 1951-1960 : The Gentleman’s agreement

1. Hagelin is at that moment the only civil manufacturer of cipher machines in the world [1]
2. AFSA considers the Hagelin Company as a serious international player
3. AFSA considers Hagelin's expanding market as a security threat
4. AFSA considers Boris Hagelin a good and loyal friend
5. Hagelin will continue to sell *readable* machines to all nations
6. The CIA will control the worldwide sale of the new secure (unreadable) CX-machines
7. Hagelin will receive **US$ 700,000** as compensation [2]
8. Hagelin will provide information about all customers and sales
9. Hagelin's offices and agents abroad may be used for information-gathering
10. Hagelin's new technology will be considered for use by NATO
11. Hagelin's OTT technology might also be of use to NATO

With respect to point (5) above, the report literally says:

> It would be to the advantage of the U.S. Government if the proposed new or improved Hagelin cryptoequipments were prevented from being developed, manufactured, and sold commercially on the open market.

| | |
|---|---|
| Egypt | Negotiating for 50 x C-52 and 10 x BC-52 |
| Jordan | 10 x C-52, 20 x BC-52 (UK is paying for this order) |
| Iran | No agent, no interest |
| Iraq | Negotiating for 50 to 200 x C-52 with Arabic characters |
| Syria | 50 x C-36 [1] |
| Saudi Arabia | No agent, no sales yet |
| India | Interested in C-52 and BC-52 |
| Pakistan | Waiting for C-52 for Hindustani (29 or 30 characters) |
| Belgium | 200+ x CX-52a, 100 variable type wheels for C-446 |
| France | 80 x CX-52a, 20 x CX-52a/10 (for study), interested in HX |
| Portugal | 5 x CX-52a |
| Italy | Awaiting NATO viewpoint on CX-52 |
| Greece and Turkey | Interested, documentation sent. Trip postponed. |
| Holland | 500 to 1000 x C-446, some with OTT (C-446/RT) |
| Dutch Army | Interest in CX-52 and BCX-52. |
| United Kingdom | 2 x CX-52 |
| Germany and Austria | H-54 supplied by HELL (CX-52bk) [2] |
| Sweden | Will replace their C-446 by CX-52 units (long-term) |
| Spain | Interested in C-52, no orders yet |
| Eire | 2 x CX-52 |
| Indonesia | 20 to 30 x C-52 (waiting for order) |
| Poland and Hungary | 2 x C-446 each [3] |
| Jugoslavia | Interested in C-machines [4] |
| Central America | Not much interest (see below) |
| Costa Rica | 2 x C-446 |
| Cuba | Initially interested, but no sales |
| Mexico | Currently trying to raise interest |
| Venezuela | About to order some machines |
| Brazil | 60 x CX-52c, interested in 500 more |
| Argentine | 13 x CX-52c |
| Chile | Not much interest, will buy some |
| Peru | Interested in 200 x CX-52 |
| Paraguay | No interest |
| Uruguay | 5 x CX-52, 2 x BC-52 (first experience with crypto) |
| Columbia | 100 x CX-52, 40 x BCX-52 |

# Opération active

- Une collaboration entre Hagelin et la NSA donne naissance à la H-460 qui contient des backdoors pour laisser la possibilité aux Etat-Unis d'intercepter les messages.
- Cette collaboration vient de l'amitié entre Friedman et Hagelin

  On parle de plus de 52 000 documents déclassifiés

H-460

# Nouveau propriétaire

Friedman malade depuis quelque année meurt en 1969 et Hagelin a maintenant 80ans. Il commence à réfléchir à son successeur : son fils Boris Hagelin Jr (Bo Hagelin)

La CIA et BND rachète Crypto AG pour 5,750,000$, change le comité de direction et fait venir de nouveaux investisseurs : Siemens et Motorola

Crypto AG passe d'un chiffre d'affaire de 15M CHF à 51M en 5ans et compte maintenant 250 employés.

Qui dit succès commerciale, dit succès de l'espionnage...

# Les doutes

Au fil des années, de plus en plus d’ingénieur de Crypto AG on des doutes vis à vis des failles béantes de leurs machines.

En 1977, un employé propose au Syriens de réparer les failles des machines.

Pour calmer les ingénieurs devenu trop bavard, la CIA recrute Kjell-Ove Widman (Henri)

En 1992, un employé de Crypto AG est retenu en otage pendant 9mois par l’Iran

Hans Bühler

C’est suite à cette emprisonnement que Crypto AG commencera sa chute.

En effet, Hans Bühler, n’est pas content et fait part de ses doutes sur Crypto AG au média suisse. L’affaire éclate et de nombreux article montrant l’implication d’agent de la CIA dans l’entreprise feront leurs apparition. Suite au scandale de nombreux employés quitteront ainsi la boite, mais surtout beaucoup de clients rompent leurs contrats (l’Arabie Saoudite, l’Argentine, …)

En 1992, l’Allemagne ayant peur des répercussions si on les relie à l’affaire décide de vendre leurs parts à la CIA pour 17M $

Les nouvelles technologies, la mauvaise gestions de l’entreprise et la mauvaise réputation signera la fin définitive de Crypto AG en 2017

# Sources


- CryptoMuseum, consulté le 17/04/22, https://www.cryptomuseum.com/manuf/crypto/index.htm
- Greg Miller, The Washington Post, 11/02/20, consulté le 17/04/22, https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/
- Opération Rubicon : Espionnage à l’échelle mondiale, https://www.youtube.com/watch?v=SWFlA248spU
- Comment la CIA a espionné le monde entier : L’Affaire Crypto AG, Sylvqin, https://www.youtube.com/watch?v=54jbXAVy_Rw

La vieille règle est toujours d’actualité : la qualité d’une machine dépend largement de son utilisateur.

The Story of the Hagelin-Cryptos, Boris Hagelin

Merci de m’avoir écouté