
# Telex-berichtbeveiliging

# De nooit onthulde Nederlandse historie op cryptografisch gebied 1945-~1965

# *Achter deze presentatie, maar dan vooraf*

- De uitvinder prof dr. ir. R.M.M. Oberman
  - PTT 1935-1957
  - TH-Delft 1958-1980 (deeltijd: 1947-1957)
  - Speurwerkprijs van PTT : 1980

- De spreker: the next generation
  - TH-Delft
  - Kon. Marine, …., PTT,
  - Communicatie-infrastructuur consultancy

# *Bronnen en… onverwachts juist geen bron*

**Bronnen**

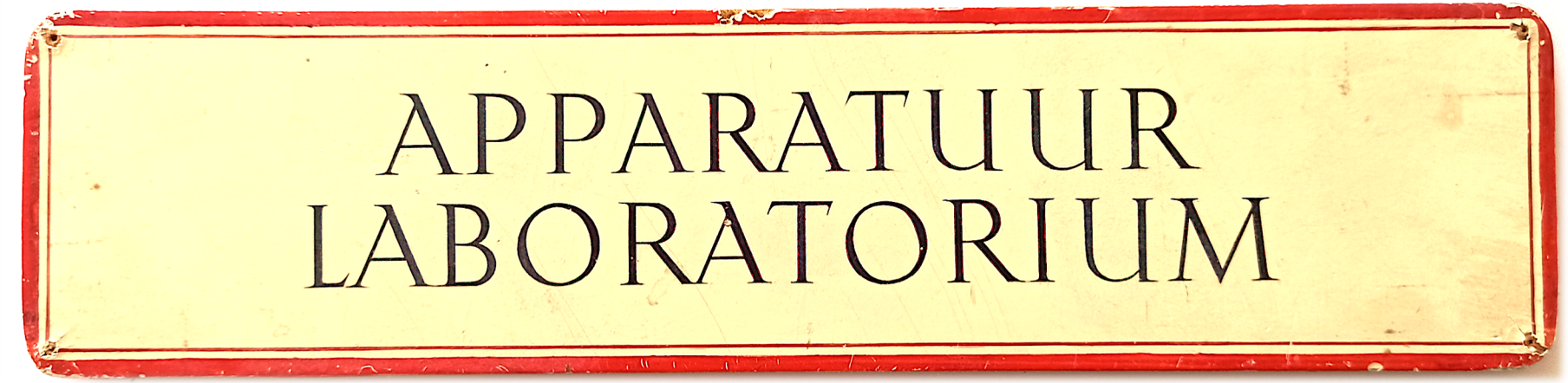
1. Nationaal Archief: 185 dozen = 0,02% NA; ±4000 p.
2. AIVD: 4 inzage verzoeken, 1 hoorzitting: ~1000 pag.
3. Privé en daardoor nooit onthulde archieven: ~400 pag.

**Juist geen bron, de PTT domeinen!**

*Niets te vinden in*:

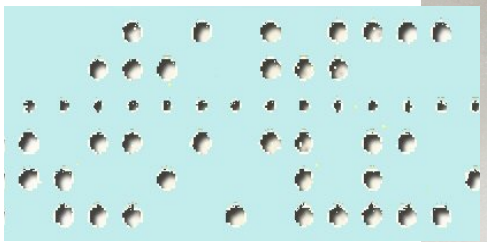
a. 100 jaar KPN research, ondanks 10 jaar crypto werk
b. KPN website over haar historie
c. …..

# KPN/Dr. Neher laboratorium:
## Waar gebeurde het cryptowerk bij PTT?



# Telex, wat was het ??????

- De email equivalent van 70 jaar geleden
- Electronisch gekoppelde typemachines
- Tekstberichten
- Invoer:
  - Toetsenbord
  - Papertape
- Eind t/m eind automatisch





www.johanneskok.com/collection_rtty/

# De aanloop 1943-1945 en verder.....

SUBJECT : Recommendations for Legion of Merit and Medal for Merit Awards

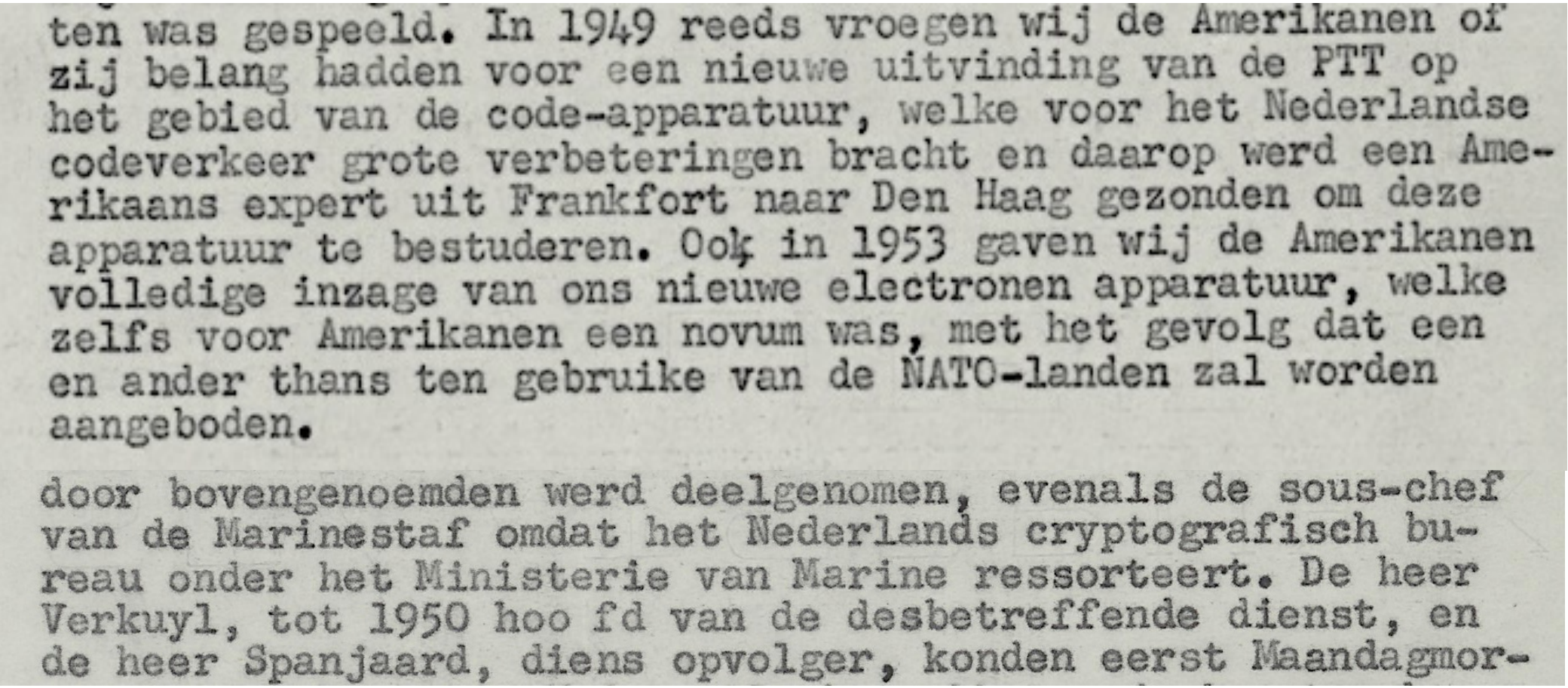
1. After much thought and careful study of the memoranda sent me by Branch Chiefs on the subject, the achievements

[19430927]

d. The next most valuable source of intelligence was the Japanese transposed code system known as "J-18" and "J-19". Its solution represented a high cryptanalytic achievement, for initially the system appeared to be impregnable. For the development of the techniques and procedures in solution and for the mechanization of those techniques and procedures major credit belongs to Major Rowlett and Messrs. Ferner and Small. For continuity in cryptanalytic operations, credit belongs to the group under the direction of Colonel J. A. Verkuyl, including Mr. Eugene Waltz, Mr. William O. Bryan, Mr. Joseph S. Petersen, Jr., Mr. (now Sgt.) George Hurley, Miss Isabel M. Murdock, and Miss Elizabeth Stevens.

**SIS, 1943**

# Verkuyl – Petersen affaire, 1954.....



ten was gespeeld. In 1949 reeds vroegen wij de Amerikanen of zij belang hadden voor een nieuwe uitvinding van de PTT op het gebied van de code-apparatuur, welke voor het Nederlandse codeverkeer grote verbeteringen bracht en daarop werd een Amerikaans expert uit Frankfort naar Den Haag gezonden om deze apparatuur te bestuderen. Ook in 1953 gaven wij de Amerikanen volledige inzage van ons nieuwe electronen apparatuur, welke zelfs voor Amerikanen een novum was, met het gevolg dat een en ander thans ten gebruike van de NATO-landen zal worden aangeboden.

door bovengenoemden werd deelgenomen, evenals de sous-chef van de Marinestaf omdat het Nederlands cryptografisch bureau onder het Ministerie van Marine ressorteert. De heer Verkuyl, tot 1950 hoo fd van de desbetreffende dienst, en de heer Spanjaard, diens opvolger, konden eerst Maandagmor-

[19541012]

1. CCB/ MARID VI had baat bij alle bondgenootschappelijke info
2. Info was wederzijds….

# Terug naar ±1945: Cryptografie *en* Crypto-analyse

- *Cryptografie* in die tijd => de Nederlandse regering:
  a. Ministerie van Buitenlandse Zaken
  b. Koninklijke Marine

- *Crypto-analyse in het belang van de NL regering*
- Wereldwijde politieke inzichten en voorspellingen
  i. Economische spionage
  ii. Stimulering van crypto export

- **Niemand is je vriend** in the crypto-analyse wereld

# Telex berichtbeveiliging ±1946, maar wie?

- BUZA vroeg PTT: ontwerp en maak telex **crypto**systeem

1. Telex was het enige internationale E-berichtennetwerk.
   - Telex was de electronic mail van toen…

2. Telex en de kennis was PTT monopolie en expertise
3. PTT was onderdeel van de overheid, dus vertrouwd
4. Cryptografie was geen deel van PTT als netwerk bedrijf
5. PTT was technologisch geïnspireerd, niet politiek

5 September 1946 No. 113 Kabinet.

MINISTERIE VAN
BUITENLANDSCHE ZAKEN

'S-GRAVENHAGE, den 5den September 1946.

AFDEELING Verbindingen.

No. 275.

Men wordt verzocht bij de aanhaling van dezen brief dagteekening, nummer en afdeeling nauwkeurig te vermelden

Korte Vijverberg 5

Tel. 180309

Hiermede moge ik Uw aandacht en medewerking voor de volgende aangelegenheid verzoeken.

Zooals U bekend zal zijn beschikt de Afdeeling Verbindingen van mijn Ministerie over een telexcentrale, waarop thans Hr. Ms. Ambassades te Londen en Parijs en binnenkort, naar verwacht mag worden, ook andere posten in het buitenland zullen worden aangesloten.

Daar een groot gedeelte van het verkeer met het buitenland in code gesteld is, werd de mogelijkheid onder de oogen gezien om door middel van de telexapparatuur een systeem van codeering te ontwikkelen, waardoor een extra bewerking zou kunnen worden uitgespaard en wellicht een doeltreffend systeem van versluiering kan worden bereikt.

— Het originele verzoek van BUZA in september 1946 aan PTT
Telex was net geïnstalleerd: ambassades van Londen and Parijs

# Wie deed wat in 1946 en 1947

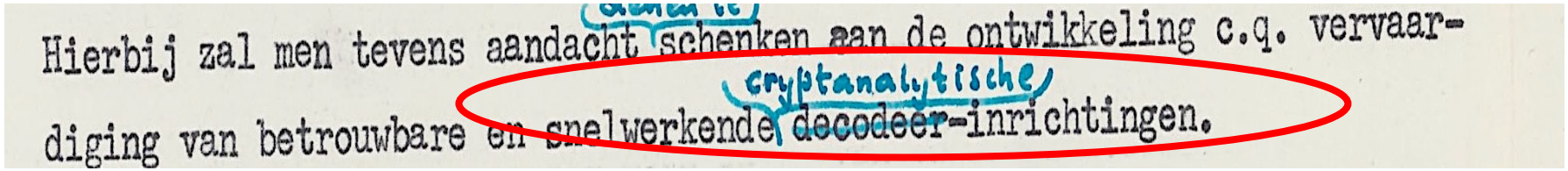
1. PTT: Dr. Neher lab: Apparatuur Laboratorium: Oberman
2. PTT: Vercijferapparaat voor *Telex berichtenverkeer:* ***Colex***
   a. Sleutelgenerator
   b. Mixer
   c. Koppeling met het Telexnetwerk
   ➢ ±12 maanden doorlooptijd

3. *BuZa was de opdrachtgever en de eerste afnemer*
   - *De KM volgde daarna*
4. Code Coördinatie Bureau: Colex evaluatie (Verkuyl)
5. Verkuyl: was ook hoofd van Marid VI……

6. De Colex was in het najaar van 1948 al operationeel

# Wat is: One Time Pad, OTP

1. Theorema van Shannon: witte ruis …. is de ”sleutel” tot…
2. OTP sleutelproductie: Duplicatie en sleutelcontrole en ? ☺
3. Oproep in 1953 door O. voor brede overheids-support


Hierbij zal men tevens aandacht schenken aan de ontwikkeling c.q. vervaar-
diging van betrouwbare en snelwerkende cryptanalytische decodeer-inrichtingen.

4. 

Statistiekcontrole op de OTP-sleutelproductie= ….

5. CCB bestelde in 1954 een statistiek machine; doel: crypto-analyse.

# Colex, de techniek, …….

1. De Roulette, de sleutelgenerator……
2. De Mixer: eerste ontwerp 60 relais, finale ontwerp 98 + 2

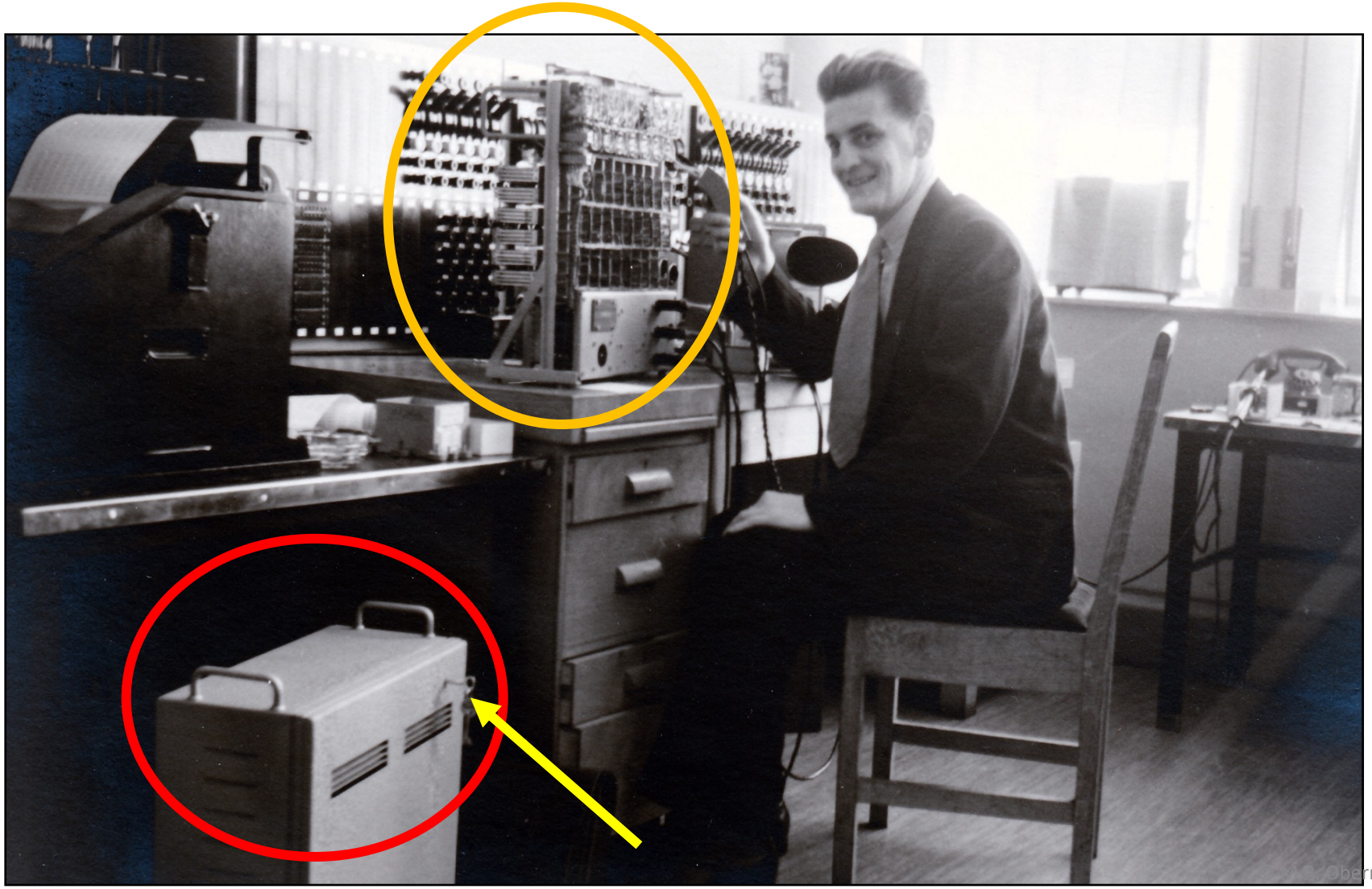
- Eerste ontwerp geoptimaliseerd: minimalisatie van de relais
- Derde ontwerp: onderhoudbaarheid: identieke relais ipv min.

❖Beschikbaar: 1200 relais t.b.v. 12 systemen

❖Gebruikt: 600 ⇢ Londen, Parijs, Washington, Batavia, Den Haag (2)

✓ ARCO: 600

# 1947-1948: De Colex : **Co~~dete~~lex**



# De formele indienststelling: 5 april **1949**

W. Drees

Mede-afdoening van:

*Aan* Washington
Londen
Parys

over

Voor Ambassadeur persoonlyk stop In tegenwoordigheid van allen die een belangryk aandeel hebben gehad in de ontwikkeling van deze nieuwe codeerinrichting cma thans byeengekomen voor de formele indienststelling daarvan cma moge ik U gelukwensen met het bezit van deze apparatuur cma welke een onschatbare stapx voorwaarts betekent in de geheime berichtenwisseling tussen U en de Nederlandse Regering stop Ik ben ervan overtuigd cma dat de verwezenlyking van dit project dank zy de uitvolprezen medewerking van de P.T.T. cma voor Nederland van eminent belang zal blyken te zyn stop Drees.

Gecoll.

BIJLAGEN

te weten:

W. Drees

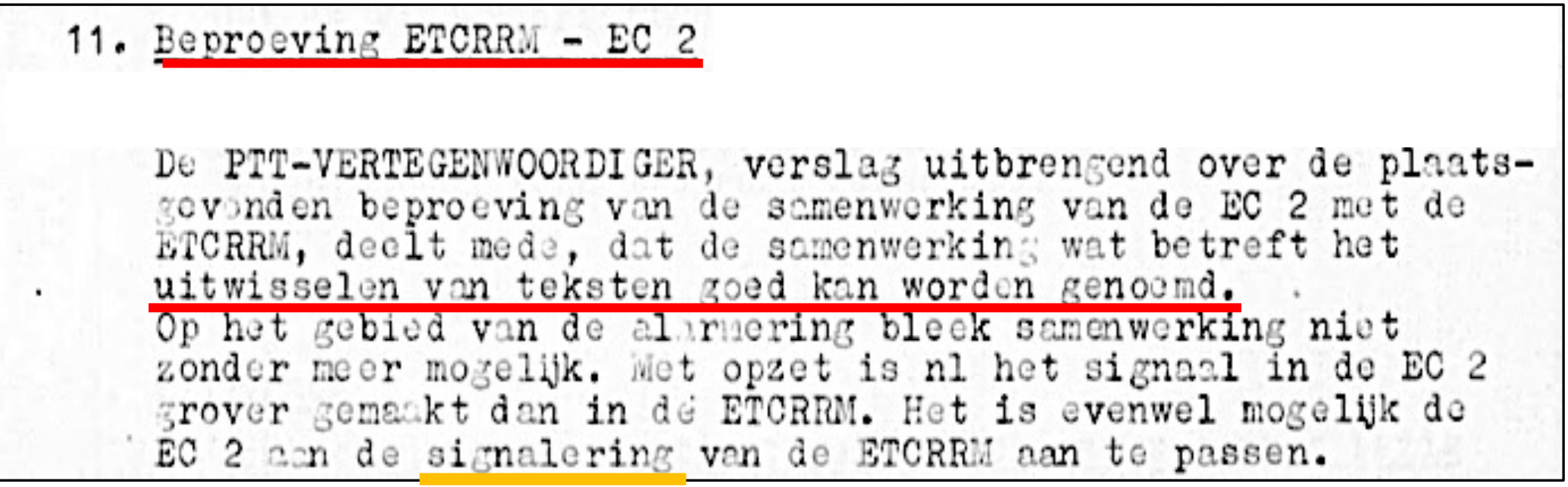
# Het succes: 1946-1957

- De Colex, relais 1947, 3-6 tekens/s
- De Ecolex; radiobuizen, 1950:40 tekens/s
- De Ecolex II: transistoren 1956
- De PTT mensen waren zeer gemotiveerd
- Blije klanten: BUZA, **KM,** ….☺

- De PTT-top, dg, dacht er anders over……(1952) ☹

# OTP, de Ecolex II in het internationale veld..

- Samenwerking van verschillende OTP systemen?
- Ja, mits……

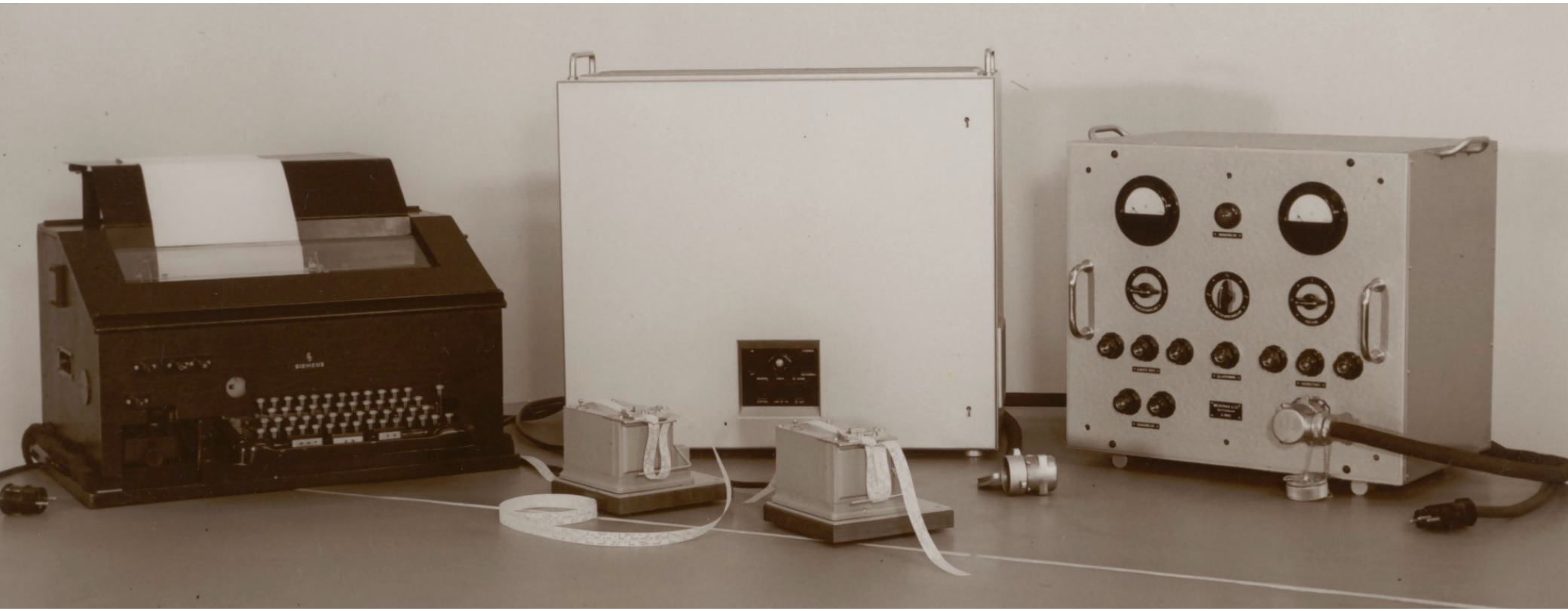


11. Beproeving ETCRRM - EC 2

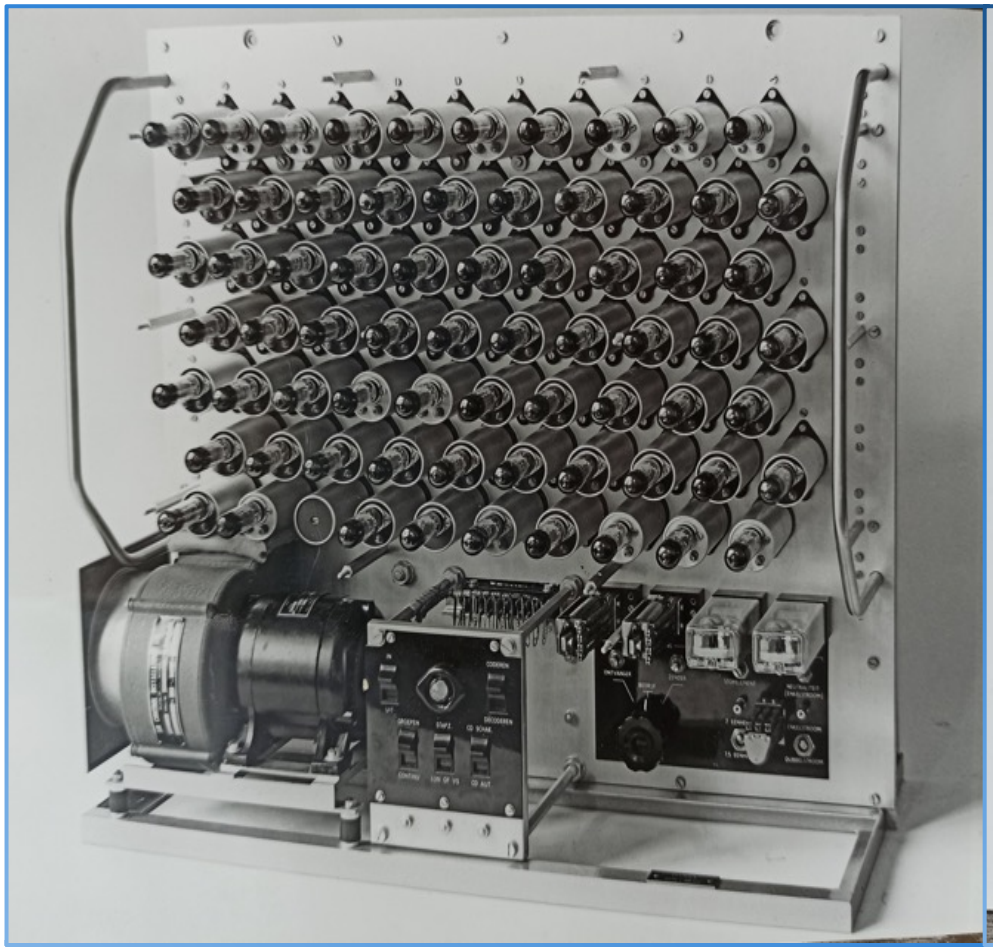
De PTT-VERTEGENWOORDIGER, verslag uitbrengend over de plaatsgevonden beproeving van de samenwerking van de EC 2 met de ETCRRM, deelt mede, dat de samenwerking wat betreft het uitwisselen van teksten goed kan worden genoemd.
Op het gebied van de alarmering bleek samenwerking niet zonder meer mogelijk. Met opzet is nl het signaal in de EC 2 grover gemaakt dan in de ETCRRM. Het is evenwel mogelijk de EC 2 aan de signalering van de ETCRRM aan te passen.

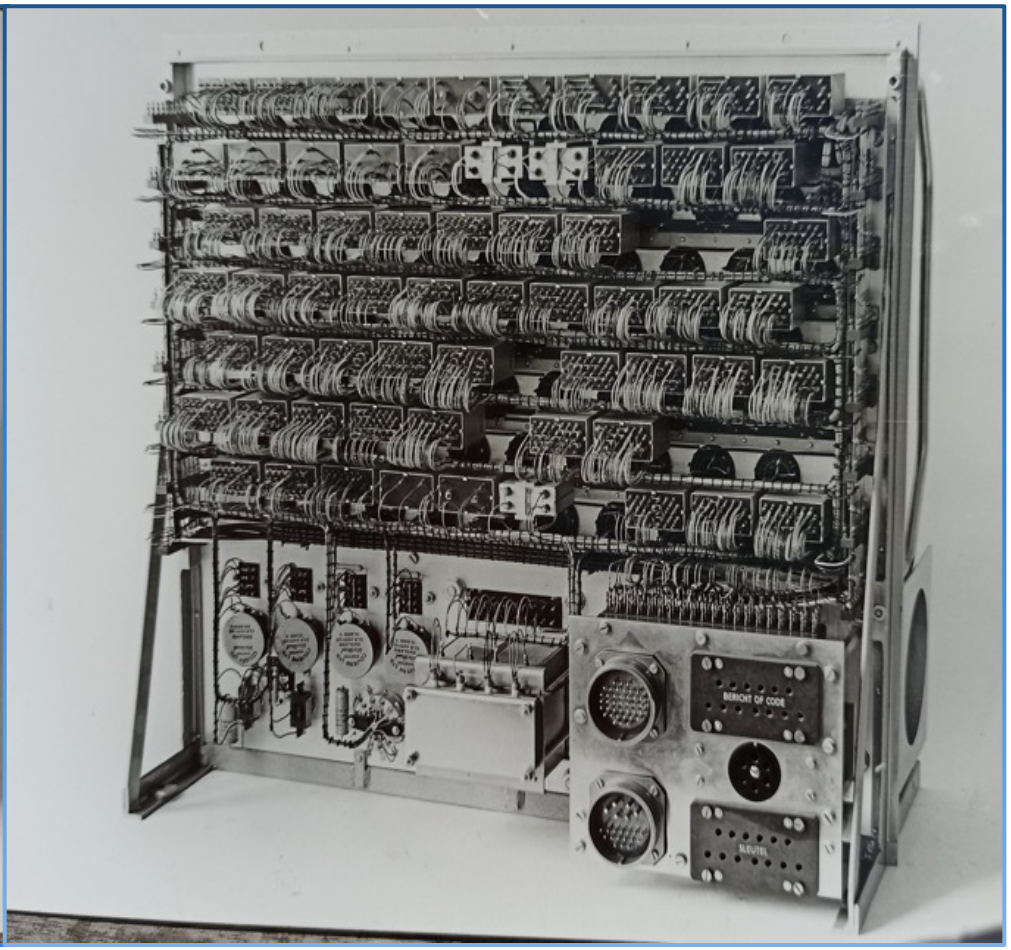

- ETCRRM: Noors OTP systeem….. Radiobuizen en relais
- Commercieel interessant: veel soorten OTP-systemen
- Samenwerking verschillende OTP-systemen *<u>is</u>* mogelijk!

# Een Ecolex-opstelling

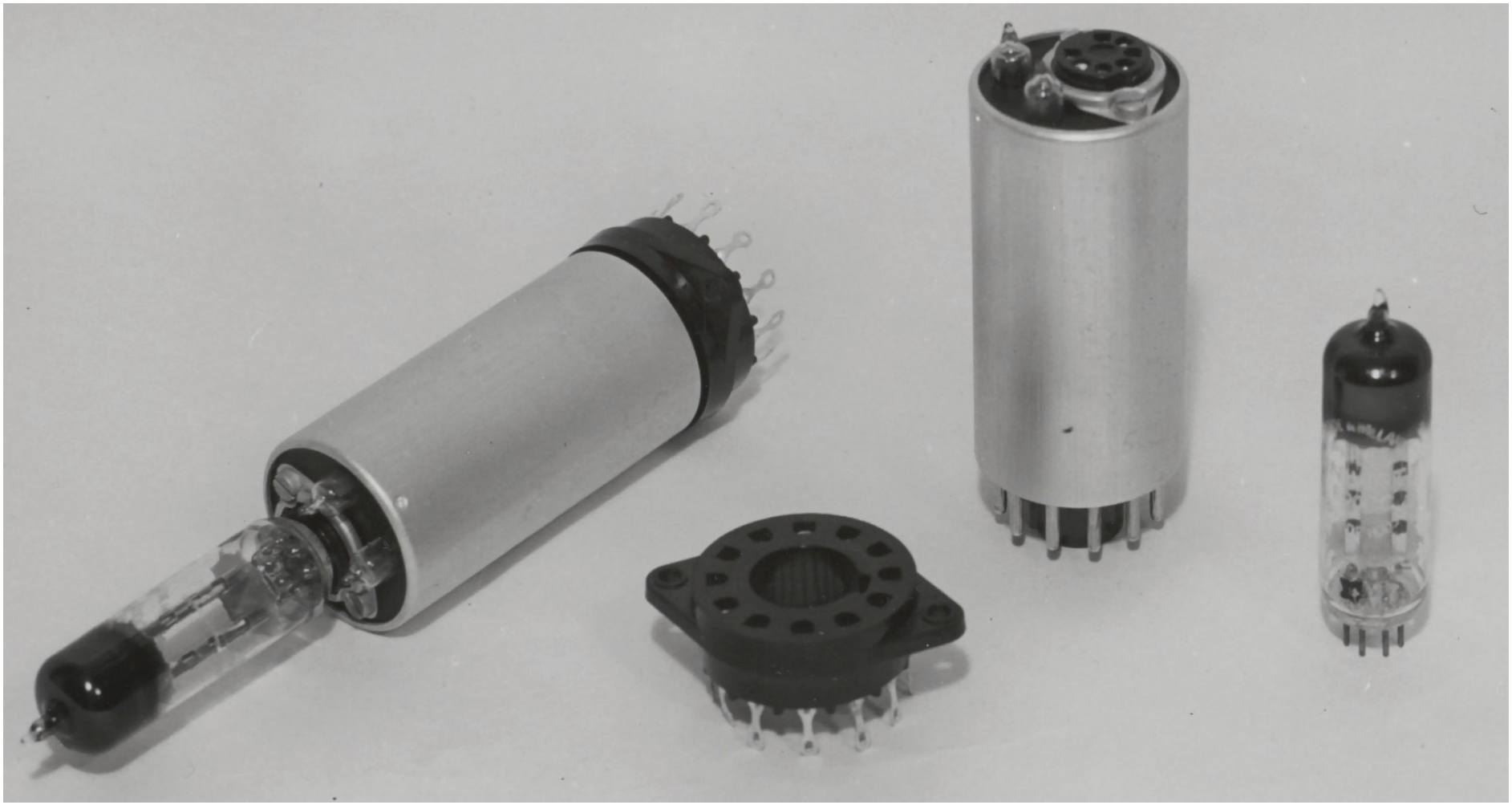


# Ecolex: radiobuizen





# De Ecolex: radiobuizen en opzetvoetjes



# De worstelingen 1946-1957

- De DG was (maar intern **niet** … ) blij met het succes ….
- Er waren weinigen die wisten wat Oberman c.s. deden
- De Colex was gebaseerd op: **security by obscurity**
- Oberman's team werd betaald voor het Colex succes:
  - "Gemis aan octrooi ……."
  - Vergoeding BuZa, de basisbesparingen voor BuZa
  - BuZa was de funder, niet PTT!
  - De betaling was *buiten* de controle, van PTT !!!

- De DG wilde van crypto af …., al in 1952; …..

# Onderhandelingen PTT - Philips USFA: 1952 >

1. PTT: vertegenwoordigde de Staat … >…Henro… ☺/☹
2. KM noch BuZa hadden trek in het vertrek van PTT…
3. PTT: 7,5% gerelateerde USFA omzet t.b.v. onderzoek ☹
4. Contract pas 5 > jaar na DG initiatief: **september 1957**

**Contract issues:**

- BuZa/KM handen vrij, onderdelen voor installed base

# Na de scheiding van PTT in 1957

**1957-1959**

1. Oberman ging naar de TU-Delft, maar niet alleen….
2. In 2 jaar volgden 10 van de 13 voormalige teamleden
3. USFA ontving geen support van PTT, (er was niemand meer …)
4. Oberman – USFA onderhandelingen waren niet succesvol

**<u>Zes</u> jaar na de PTT exit:**

➢Ecolex IV: 1ste systeem ontwikkeld door USFA

➢De transfer van PTT naar USFA was een ramp…..!!!

# Andere “PTT-USFA” scheidingseffecten:
## *een nieuwe partner 1960-1965 voor O/S*

- Oberman kreeg een ontwikkelingscontract: NVBR/NBV ±1962
  - NBV was achterdochtig t.a.v. een commerciële partij!
  - NBV meende dat USFA hun wensen onvoldoende zag

- Het contract eindigde in 1965 door gebrek aan USFA samenwerking  met het NVBR, (O/S)
  - Resultaten: o.a. een **zelf**-permuterend cryptosysteem
  - Systeem getest en gecertificeerd door het  NBV/NVBR

- USFA had zijn eigen weg gekozen!
- Een NBV goedgekeurd systeem was onvoldoende voor USFA

# Cryptografie en –analyse in NL na WW-II

1. Crypto policy
   - CCB 1946-1960;
   - eerste jaren CCB <-> MARID VI
   - NVBR/NBV 1960 →, ☺
2. Crypto-praktijk: Marid-VI: interceptie en analyse
3. Internationaal CA overleg: selectieve landen

➢ Deelname, alleen als je kennis**inbreng** had ……

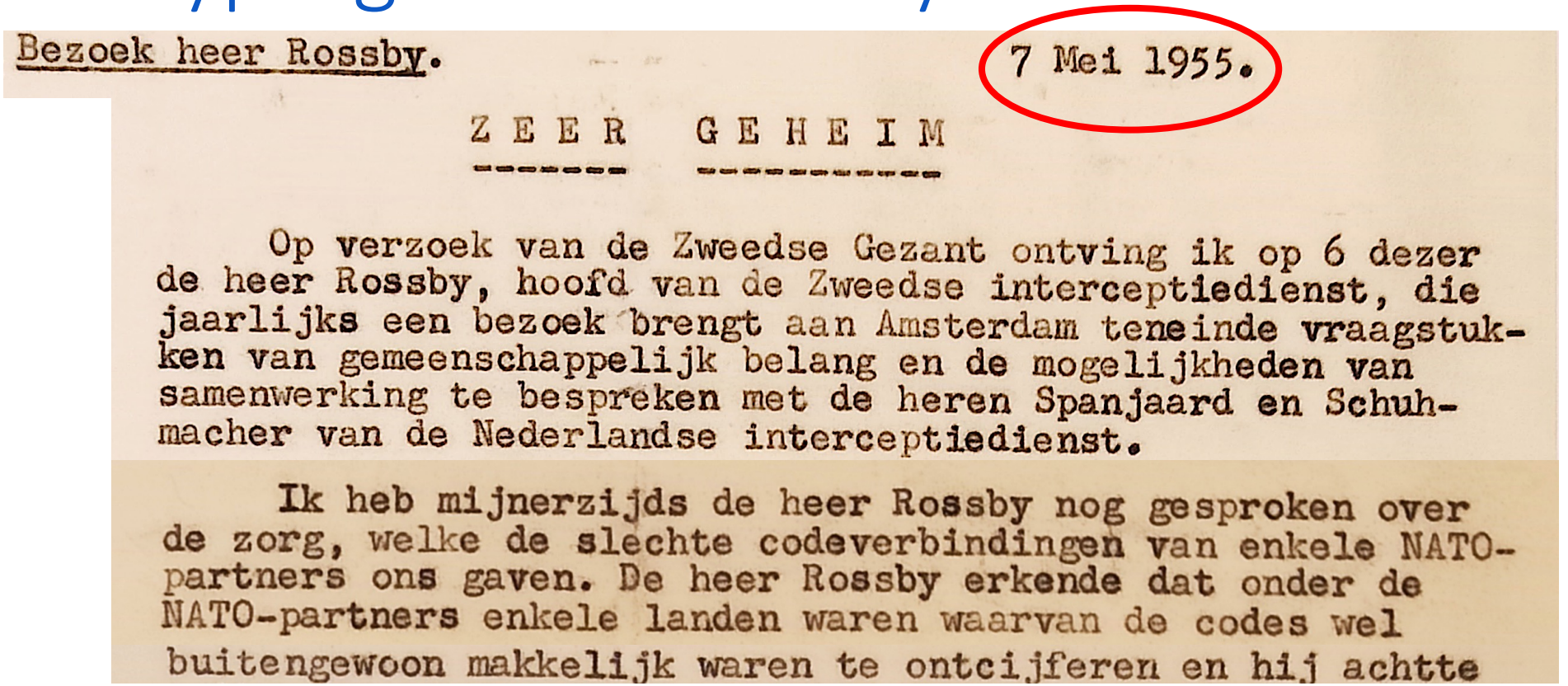
# Even de actualiteit van nu: **Crypto-Analyse**

1. **Politie,** hack-resultaten van **berichten**diensten:

   - 2016 Ennetcom
   - 2018 Phantom Secure
   - 2019 PGP Safe,
   - 2020 EncroChat
   - 2021 Sky ECC, **ANOM**, ……
   - **2023** Exclu Messenger

2. Oekraïne, de gevolgen van GSM-gebruik…

# Cryptografie en -analyse in Nederland



Bezoek heer Rossby. 7 Mei 1955.

ZEER GEHEIM

Op verzoek van de Zweedse Gezant ontving ik op 6 dezer de heer Rossby, hoofd van de Zweedse interceptiedienst, die jaarlijks een bezoek brengt aan Amsterdam teneinde vraagstukken van gemeenschappelijk belang en de mogelijkheden van samenwerking te bespreken met de heren Spanjaard en Schuhmacher van de Nederlandse interceptiedienst.

Ik heb mijnerzijds de heer Rossby nog gesproken over de zorg, welke de slechte codeverbindingen van enkele NATO-partners ons gaven. De heer Rossby erkende dat onder de NATO-partners enkele landen waren waarvan de codes wel buitengewoon makkelijk waren te ontcijferen en hij achtte

**Zweden bezoekt Marid-VI**: een voorloper van …..

1. Internationale samenwerking, … toen al!
2. Zweedse opmerkingen over de NATO communicatie
3. En enkele andere landen ☺☺

# “Niet-technisch”: Interceptie en crypto-analyse….

- Interceptie na WO-II:
  - Eemnes, Voorburg, KM schepen, later ook nog  Burum

- Crypto-analyse
  1. Veel landen waren door NL meeleesbaar (>70):…..
  2. Politiek en invloed
  3. Economische belangen elders
  4. Eigen evaluatie  t.b.v. “zelfkennis”
  5. Crypto-apparatuur: Export versus nationaal belang (zie 1)
  6. Verkoop (5) voorkomt wellicht onbreekbare systemen (zie 1)

# 1952: Oberman en Verkuyl bezochten Hagelin: Sweden

Het principe waarop de vercijfering door de CX-52 crypto-
graaf berust wijkt sterk af van dat der vroeger gebouwde machines,
omdat de pinwielen afzonderlijk en onregelmatig draaien. Hieruit
volgt, dat alle tot heden bekende analytische methoden, die, dank
zij het constant en gelijktijdig verplaatsen der zes pinwielen
van de vroeger typen machines, met succes op de crypto teksten
konden worden toegepast, onbruikbaar zijn geworden voor decrypte-
ring van de door de CX-52 geproduceerde berichten.

Het fragment bedoelde te zeggen!:
MARID VI, kon de eerdere Hagelin machine's meelezen

# Andere historische momenten, nu opgelijnd

- 1953 Oberman bezocht Hagelin: ….1,5 uur later, …..
- 1955 Oberman bezocht  Hagelin: Rotor - shiftregister
- 1968 Briefuitwisselingen tussen Oberman and Hagelin

**Hoofdlijn:** Hagelin was niet in voor verbeteringen

Dit leidde thuis tot:

Wie is daar eigenlijk de baas

# Crypto-analyse maar dan anders: ±1978

- Van **A**roflex naar **B**eroflex
  - De wiskundige B-oplossing kwam van Marid VI
  - Marid-VI was ook de bron voor de analyse machine
  - Philips-Nijmegen chip design gereedschappen

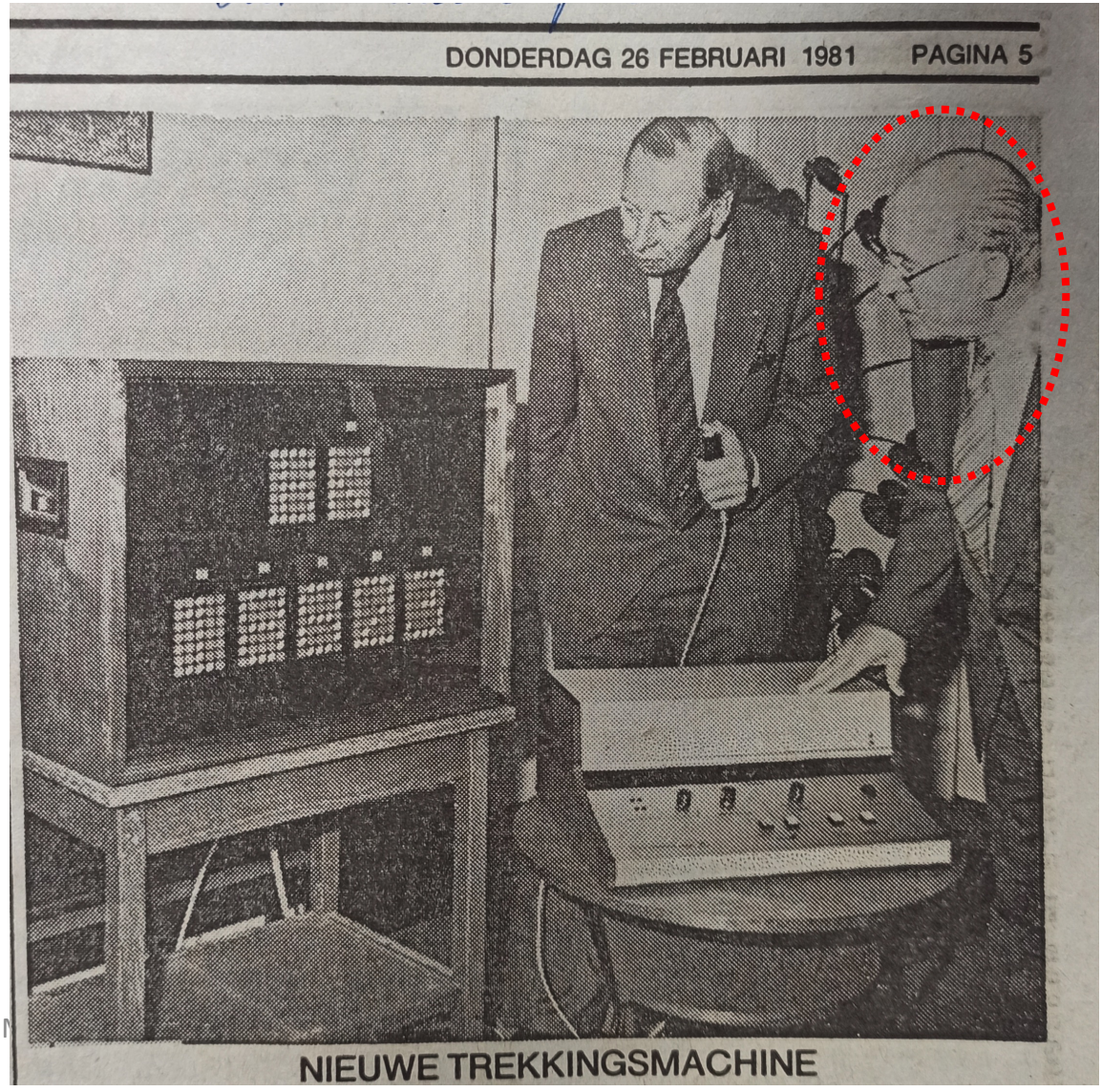
  - *Techniek:*
    - Parallel design-oplossing
    - Dedicated purpose chip 1977/78
    - Chip-design: 2 net afgestudeerde TU-Delft ir's (Marid VI)

# Een crypto-uitstapje…: De Staatsloterij….

## De kern: de sleutelgenerator van de Colex/Ecolex

1970


1981



# Terzijde 1:
# Crypto-betrokken organisaties na WO-II:

| | *Wie* | *wanneer* | *jaren…* |
|---|---|---|---|
| 1. | PTT | 1946 – 1957 | 11 |
| 2. | Philips USFA | 1957 – 1990 | 33 |
| 3. | Philips Crypto | 1990 – 2003 | 13 |
| 4. | Compumatica Secure Networks / FOX-IT | 2003 – ……. | 19+ |

# Terzijde 2:
# Crypto-betrokken organisaties na WO-II:
# Overheid

1. Code Coördinatie Bureau 1946 -1960
2. Marid VI/WKC TIVC 1946 - …

3. NVBR/NBV 1960 - ….

# *Tot slot, in 1 A4 tje ☺1946 - 1965 →*

1. PTT was cruciaal voor de nationale telex berichten beveiliging
2. Cryptografie had de hoogste nationale belangstelling
3. OTP: veilige keuze voor BuZa, Kon. Marine en ***…… W-DU/DEN***

4. **“Staatsveiligheid” was fataal voor** de continuïteit bij PTT
   - Weet niemand wat je doet, dan gaat het niet goed….

5. **De overdracht door PTT was een ramp voor Philips USFA**

6. Cryptografie was toen en nu: cruciaal voor de overheid

7. Crypto-analyse kennis is noodzakelijk ……

# Wilt U inmiddels nog meer weten…???

- De nog nooit beschreven geschiedenis
- De basis: Staatsgeheime documenten en privé archief
- ±120 Originele fragmenten
- 268 Pagina’s
- Hardcover
- www.oberman.nl/boek

Vragen: maarten@oberman.nl