

GEHEIM

NATIONALE VERBINDINGSBEVEILIGINGSRAAD
(N. V. B. R.)

1/6

Classificatie } GEHEIM
Rubricering }

Technische Werkgroep T.R.O.L.-app.

Nummer : A/3/162 (TW 3)

Ex.No. 11

Datum : 24 juli 1961

Onderwerp: Vergadering 11 juli 1961

Bijlage : één (schema)

Verslag van de derde vergadering van de technische werkgroep T.R.O.L.-
apparatuur gehouden op 11 juli 1961 te 's-Gravenhage, Plein 23.

Aanwezig: plv. voorzitter : Hr. A. Elsackers, plv. vz. NVBR
NBV/B : Hr. A. Luyt
Delftse Groep : Prof. dr. ir. R. M. M. Oberman
Hr. A. Snijders
RVO/TNO : Ir. S. Gratama
Ir. R. Slegtenhorst
Ph. Usfa N.V. : Hr. H. de Fremery
Ir. J. van Lottum
plv. secretaris : Hr. F. Hafkamp, NBV/B

1. Opening

De voorzitter deelt mede dat de heer Verdonck en de heer Versluis door vakantie verhinderd zijn en dat prof. van Soest eveneens verhinderd is.

2. Vorige notulen

Het verslag van de eerste vergadering wordt gearresteerd onder het voorbehoud, dat indien prof. Oberman opmerkingen heeft, hij deze als nog vóór 18 juli a.s. kenbaar zal maken.

Naar aanleiding van het verslag van de 2e vergadering worden de volgende opmerkingen gemaakt:

Prof. Oberman wil zien opgenomen dat hij naar aanleiding van het Memo NVBR/A/3/144 van USFA de opmerking gemaakt heeft dat het aantal transistors alleen niet maatgevend is voor een kostenvergelijking van verschillende apparaten.

De voorzitter wijst erop dat in de zin welke begint op de 13e regel van onder op pagina 1 van bedoeld verslag, EC IV moet worden veranderd in EC V. In de hierop volgende zin wordt inderdaad de EC IV bedoeld.

Hij stelt dat de heer Verdonck in afwijking van het weergegevene in de 2e alinea van de 3e pagina gezegd heeft, dat, rekening houdend met alle bekend geworden omstandigheden naar zijn persoonlijke mening de keuze zal moeten vallen op een bijzetkastje bij de EC IV.

Hij stelde voorts voor om op te nemen dat de heer de Fremery aan het slot van de vergadering gesteld heeft dat de directie van Usfa besloten had om door te gaan met de ontwikkeling van het Usfa bijzetkastje en van mening was dat die partij, die het eerst een prototype gereed had, dit ook het eerst aan SECAN diende aan te bieden; waarop de heer Verdonck had geantwoord dat een apparaat alleen dan zal worden aangeboden, wanneer de NVBR zich daarmee kan verenigen.

Na het.....

GEHEIM

Na het aanbrengen van bovenstaande wijzigingen werden ook de notulen van de tweede vergadering gearresteerd.

3. Memo Usfa betreffende cryptografische ontwikkeling ECOLEX V (NVBR/A/3/143)

Prof. Oberman stelt dat de datering van het memo zoals het aan de leden gedistribueerd is niet juist kan zijn, daar in dit memo wijzigingen verwerkt zijn, welke na de 2e vergadering zijn aangebracht; terwijl de datering van dit memo eerder dan de 2e vergadering is gesteld.

De heer de Fremery antwoordt dat de essentie van het memo door de aangebrachte wijzigingen niet is veranderd, maar dat hij zich gaarne verenigt met de bijvoeging: "gecorrigeerd dd. 10 juni 1961".

4. ECSA Serial 994

De voorzitter deelt mede, dat ECSA Serial 994 betreffende "Supreme Commanders' Requirements for On-Line Communications Security Equipments" geheel in overeenstemming is met ECSA/WP 115/4, behalve punt 9 (d), dat nu als volgt luidt:

"For broadcast working the equipment shall be capable of joining a broadcast at any time during the crypto-period, at the start of a message element, but shall not require special synchronising trans-missions".

5. "Wielenco commissie"

Op uitnodiging van de voorzitter brengt de heer Luyt verslag uit van de werkzaamheden en resultaten van de zg. "Wielenco commissie" (vide gestelde pagina 4 Verslag 2e vergadering).

De heer Luyt deelt mede dat twee wielen met verschillende eigenschappen in schema zijn gebracht. Het ontwerp van de heer Snijders is opgenomen als BWLAGE bij dit verslag.

In de commissie werd door de heer Hafkamp de mogelijkheid van een meer logische en goedkopere toepassing van het principe voor een onregelmatige vervanging naar voren gebracht, waarbij gebruik werd gemaakt van het voorgaande crypto-karakter.

Het bezwaar dat de commissie noopte tot het niet-adviseren van deze toepassing is, dat een verminkt crypto-karakter twee verminkte klare karakters oplevert.

Hoewel dit nog niet is uitgezocht, is de commissie van mening dat de onregelmatige vervanging in een bijzetkastje bij de EC IV kan worden aangebracht.

Naar aanleiding van de werkzaamheden van de Wielenco commissie werden de volgende opmerkingen gemaakt:

Prof. Oberman acht het bijzetkastje een bijzonder onaantrekkelijke verdeling voor de klant. Hij laat een waarschuwing horen aan het adres van Usfa, dat de moeilijkheden van concurrentie en analyse niet onderschat mogen worden. Hij illustreert deze moeilijkheden, waarbij hij er onder meer op wijst, dat uit publikaties is gebleken, dat men in andere landen bijzonder ver is op het gebied van recurrenente reeksen. Hij stelt dat het wenselijk ware geweest dat de Wielenco commissie tot een vaststelling in beginsel was gekomen van de eisen, welke aan een wiel gesteld dienen te worden.

De heer Luyt antwoordt dat de opdracht van de Wielenco commissie een technische en geen cryptografische was.

Prof. Oberman stelt....

Prof. Oberman stelt, dat hij niet bedoeld heeft, dat de Wielencommissie zich in een cryptografische discussie had moeten begeven, maar dat uit de bekende technieken opmerkingen over de eisen zijn vast te stellen.

De heer Luyt stelt voor de werkzaamheden van de Wielencommissie als beëindigd te beschouwen.

De heer de Fremery acht de resultaten van de Wielencommissie positief, vooral ook omdat de diverse technici van de verschillende denkwijzen en eisen kennis hebben kunnen nemen. Hij merkt op, dat Usfa geen gebruik van een van de wielen van de Wielencommissie zal maken in de huidige EC V, daar dit weinig zin heeft.

Wel zal een van de wielen toegepast kunnen worden in een toekomstige ontwikkeling.

Als antwoord op de waarschuwingen van prof. Oberman zegt de heer de Fremery, dat Usfa zich op cryptografisch gebied volledig richt naar de aanwijzingen en adviezen van NBV/B.

Hij vervolgt zijn betoog met het stellen van de vraag of een nieuwe ontwikkeling gericht moet zijn op een nieuw bijzetkastje bij de EC IV. De voorlopige conclusie van Usfa is, dat het economischer is wanneer een geheel nieuw apparaat gemaakt wordt met gebruikmaking van bestaande schakelingen. Ook in verband met nu bekende gegevens en eisen zal een veel beter produkt kunnen ontstaan.

In dit verband is de heer de Fremery dan ook van mening dat de werkzaamheden van de Wielencommissie gestaakt kunnen worden omdat een nieuwe fase is aangebroken, waarbij de noodzaak naar voren komt van het vaststellen van een volledig nieuw ontwikkelingsplan, los van bestaande apparaten. Daarna kan de detaillering, welke tot een prototype leidt, bekeken worden.

6. Nieuwe ontwikkeling

De voorzitter stelt dat er aldus drie apparaten zullen komen:

- a. Usfa bijzetkastje,
- b. Cryptaephyl,
- c. Een zelfstandige T.R.O.L. gebaseerd op ideeën van Delft/NBV/B.

Hij kan zich hiermede accoord verklaren, mits ieder van deze apparaten voldoet aan de eisen en speciaal aan de eis van "high grade security".

Prof. Oberman uit zijn vrees dat waarschijnlijk het bijzet-apparaat Usfa een allegaartje zal worden dat geen schijn van kans zal hebben tegen de geraffineerde concurrentie.

De concurrentie kan heel listig doen met recurrenente reeksen en als dat het geval is kan een ieder, met wielen welke een voortstapping á la Hagelin hebben, inpakken.

De heer Luyt wil hier iets toevoegen aan zijn exposé over de Wielencommissie en zegt dat er in de commissie naar voren is gekomen dat indien er veel instelbare punten in een T.R.O.L. zijn, deze ingesteld kunnen worden met behulp van een ponskaart. Hij vraagt hierover de mening van prof. Oberman.

Prof. Oberman antwoordt dat dit kan en verwijst hierbij onder meer naar een publikatie in het IBM-journal. Ook magnetische ringen zullen volgens hem een oplossing kunnen geven in het probleem van veel instelbare punten, maar er zijn (ook in verband met straling en temperatuurconstantheid) geen direct bruikbare schakelingen aan te wijzen.

De heer Luyt stelt.....

De heer Luyt stelt dat hij door zijn contacten met alle groepen een indruk heeft gekregen van de toestand van zaken en dat deze toestand hem optimistisch stemt. Hij verwacht dat zowel het bijzetkastje Usfa als de Cryptaaphyl na aangebrachte wijzigingen aan de gestelde cryptografische eisen zullen voldoen.

Bij het nieuw te ontwikkelen apparaat moet z.i. het opvoeren van de cryptografische sterkte voorrang hebben.

Indien Usfa zijn medewerking kan verlenen aan het tot stand komen van de prototypes van dit laatste apparaat zullen drie apparaten aan de NATO kunnen worden aangeboden, variërend in prijs en variërend in cryptografische sterkte. Bovendien is dan voldaan aan de wens om onze kennis toegankelijk te doen zijn voor de NATO.

De heer de Fremery wil de eventueel aanwezige verkeerde indruk wegnemen dat Usfa geen medewerking wil verlenen aan andere projecten dan het bijzetkastje. Hij geeft aan dat de informatie betreffende het Delft/NBV/B-project zijns inziens niet in een dusdanig stadium is, dat overgegaan kan worden tot het vervaardigen van een prototype.

In aansluiting op de voorstellen van de heer Luyt deelt de heer de Fremery mede, dat Usfa graag wil meewerken aan een nieuwe ontwikkeling. De vraag is alleen hoe organiseren we dat. Bij Usfa zijn lopende zaken, die een volledige inzet verhinderen; terwijl het Usfa laboratorium geen specifiek ontwikkelingslaboratorium is, maar daarenevens andere taken heeft.

Hij deelt mede dat hem door SHAPE is gevraagd:

"Indien wij een bidding organiseren in juli 1962, doen jullie dan mee?" waaruit hij de conclusie heeft getrokken dat de bidding in juli 1962 zal plaatsvinden.

Verder deelt hij mee dat een functionaris van SHAPE hem als persoonlijke en vrijblijvende mening te kennen heeft gegeven dat de praktisch acceptabele prijs, gezien de ervaringen, hoogstens 2 á 3 maal die van de EC IV zal mogen zijn (dit komt op f.10.000 á f.15.000).

Verder is volgens ontvangen persoonlijke inlichtingen van SHAPE de term "high grade security" uit te leggen als een maat voor de tijd, welke benodigd is voor een cryptografische analyse. Dit zou volgens de opvattingen van SHAPE 45 á 60 dagen zijn voor de grootst denkbare organisatie op dit gebied.

Indien de bidding in juli 1962 plaatsvindt, dienen op dat tijdstip door SECAN goedgekeurde prototypes aanwezig te zijn.

De voorzitter stelt dat hij van mening is dat indien er drie apparaten aan de NATO worden aangeboden, deze gelijktijdig dienen te worden aangeboden.

De heer de Fremery vraagt of dit essentieel is. Kunnen de apparaten niet na elkaar en toch op tijd worden aangeboden? Is het niet mogelijk de aanbidding gefaseerd te doen geschieden zoals in vorige vergaderingen ter sprake is gekomen, eerst het blokschema en later de prototypes.

Prof. Oberman wenst nog op te merken dat de N.V. Philips Usfa in de afgelopen periode van 24 november 1960 tot vrij kort geleden zich niet heeft verdiept in wat aan goede beginselen ter tafel is gekomen daarbij in het midden latend op welke datum dit voor N.V. Usfa werkelijk mogelijk geweest zou zijn. Het zou naar zijn mening mogelijk geweest zijn ook een eventueel bijzet-apparaat van een goed "permutatiehart" te voorzien indien Philips Usfa niet in de mening had verkeerd het met hun vinding bij het juiste eind te hebben.

De heer de Fremery.....

De heer de Fremery bestrijdt deze opvatting met de opmerking dat pas in het recente verleden meer concrete gegevens over de ideeën van de anderen bekend zijn geworden.

Prof. Oberman stelt dat maanden geleden een prototype van een wiel op tafel is gekomen en dat toen bepaalde eigenschappen van het ideaal lijkende wiel zijn vastgelegd. Hij maakt de opmerking dat Usfa toen niet rustig op een stoel is gaan zitten om de voor- en nadelen van het een en ander af te wegen.

De heer van Lottum stelt dat hij de vaste omtrek van het onderhavige wiel nadelig acht, doch dat zij wel in overleg met afdeling B doende zijn met wielen van grotere omtrek en een onregelmatige voortstapping.

Prof. Oberman antwoordt, dat het niet om de vaste omtrek gaat, maar om de gelijke lengte van alle wielen en de toe te passen voortstapping.

De voorzitter stelt dat het verleden goed is om er een les uit te trekken; hij zou gaarne zien dat vanmiddag beslissingen worden genomen om te komen tot een goed apparaat.

Als antwoord op de eerder door de heer de Fremery gestelde vraag met betrekking tot het gefaseerd indienen van de diverse apparaten, merkt hij op, dat inderdaad naar zijn mening gelijktijdige indiening van de prototypes niet als eis behoeft te worden gezien. Welechter zouden met de aanbieding van het eerste prototype de formules, beschrijvingen en blokschema's van de overige apparaten moeten worden ingediend. Een en ander mede in het licht van het door de heer Versluis met SECAN gevoerde overleg.

De heer Gratama memoreert dat RVO-TNO een opdracht van de KL heeft waar niet van afgeweken kan worden. Persoonlijk betreurt hij het, dat niet jaren geleden een betere samenwerking op dit specifieke terrein tot stand is gekomen.

Overwogen wordt (na eventueel contact met Delft) de Delftse wielen in de Cryptaaphyl toe te passen. Overigens ziet hij tot zijn spijt geen kans ruimere hulp te bieden bij de ontwikkeling van de nieuwe apparatuur.

7. Realisering van nieuw te ontwikkelen apparatuur

De voorzitter stelt de vraag ter discussie hoe tot de realisering van de nieuw te ontwikkelen apparatuur kan worden gekomen. In de discussie worden de voorstellen overwogen om de realisatie plaats te doen vinden bij RVO-TNO na gereedkoming van de prototypes van de Cryptaaphyl en ook om bij de realisatie het PTT laboratorium te Leidschendam in te schakelen. Beide mogelijkheden worden afgewezen.

De heer Luyt zegt dat de heer Hafkamp enige dagen per week actief aan de ontwikkeling van prototypes kan medewerken.

Prof. Oberman stelt dat de medewerking van de heer Snijders bij de realisatie verkregen kan worden.

De heer de Fremery stelt dat Usfa eind september a.s. met het maken van de prototypes kan beginnen. Het voorafgaande "denkwerk" moet echter elders geschieden.

De heer Snijders zegt zijn medewerking toe.

De heer de Fremery stelt de principiële vraag of de nieuwe ontwikkeling in de richting van een bijzetkastje of in de richting van een geheel nieuw apparaat gaat.

De vergadering.....

GEHEIM

De vergadering is unaniem van oordeel dat een geheel nieuw apparaat dient te worden ontwikkeld.

De heer de Fremery ondersteunt de idee dat bij de nieuwe ontwikkeling niet in de eerste plaats op de economische eisen maar op de cryptografische eisen dient te worden gelet.

Door de vergadering worden de heren Luyt, Snijders en Hafkamp in een nieuw op te richten commissie benoemd met de heer van Lottum als technisch adviseur.

De taak van deze commissie zal zijn de ontwikkeling in een dusdanig stadium te brengen dat medio september a.s. met de aanmaak van twee prototypes kan worden begonnen.

Prof. Oberman geeft aan de nieuw op te richten commissie de aanbeveling de onregelmatige vervanging zowel in afhankelijkheid van het voorgaande de crypto-karakter als in afhankelijkheid van het klare karakter te bekijken. Misschien zal tot een apparaat gekomen kunnen worden waarin door uitwisseling van platen de beide mogelijkheden zijn verwerkt.

8. Conclusies

De voorzitter concludeert:

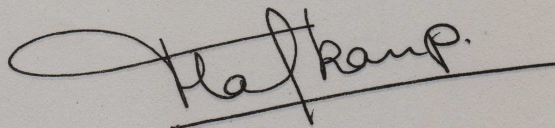
- 1) Zowel Usfa als RVO-TNO gaan door met de ontwikkeling van hun eigen apparaat, waarbij nauw contact met NBV/B zal worden onderhouden.
- 2) Er is een sub-commissie voor de verdere ontwikkeling van het Delft/NBV/B-project geïnstalleerd.
- 3) De vaststelling van de volgende vergadering zal plaats vinden op een tijdstip dat de onder 2) bedoelde sub-commissie nieuwe gegevens kan aanbieden of waarop dit om andere redenen wenselijk is.

9. Rondvraag

10. Sluiting

De voorzitter sluit de vergadering met een woord van dank aan de aanwezigen.

De plv. secretaris,



F. Hafkamp,
NBV/B

GEHEIM