GEHEIM

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

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

Classificatie)
Rubricering): GEHEIM

Nummer : A/3/148 (TW 2)

Datum : 26 juni 1961

Ex.No.: 11

Onderwerp : Vergadering 9 juni 1961.

Kort verslag van de tweede vergadering van de technische werkgroep T.R.O.L.-apparatuur gehouden op 9 juni 1961 te 's-Gravenhage, Plein 23.

Aanwezig:	voorzitter	: Hr. L.F. Verdonck, vz. NVBR, Hr. A. Elsakkers, plv. vz. NVBR,
	NBV/B	: Hr. A. Luyt, Hr. F. Hafkamp, Hr. D.B. Freelink,
	Delftse Groep	: Hr. A. Snijders, Prof.Dr.Ir. R.M.M. Oberman,
	RVO-TNO	: Prof.Dr.Ir. J.L. van Soest, Ir. R. Slegtenhorst, Ir. S. Gratama,
	Ph.Usfa N.V.	: Hr. H. de Fremery, Ir. J. van Lottum,
	secretaris	: KLTZSD J.A. Versluis, secr. NVBR.

De voorzitter opent de vergadering om 10.05 uur en heet met name de heren Oberman en Gratama welkom, die de vorige maal niet aanwezig waren. Dr. van Wijk wordt ook dit keer vertegenwoordigd door de heer de Fremery.

Voorzitter vraagt het commentaar van de heren op het memo van de afd. B (NVBR A/3/138).

De heer de Fremery zegt dat men in de afgelopen week alle aspecten van het TROL ontwikkelingsprobleem heeft bekeken. Naar aanleiding daarvan heeft hij 2 memo's opgesteld, die rondgedeeld worden (NVBR A/3/143 en 144). Hij licht deze stukken mondeling toe en komt tot de conclusie dat men zich nu niet moet gaan vastleggen op 1 oplossing. Hij geeft vervolgens de overwegingen die bij USFA gegolden hebben om de ECOLEX IV de hoogste prioriteit voor ontwikkeling te geven. Deze zijn voornamelijk van economische aard, immers moet het voor de bezitters van de ECOLEX IV aantrekkelijk zijn, om hiervan door het bijkopen van een voorzet-apparaat, een T.R.O.L.-machine te verkrijgen. SHAPE werd dan ook reeds deze mogelijke oplossing in het vooruitzicht gesteld. De heer de Fremery herhaalt vervolgens de ideeën van USFA die ook reeds bij de 1e vergadering naar voren werden gebracht.

De voorzitter vindt dat noch de ontwikkelingstijden noch de geschatte prijzen er moedgevend uitzien. Tav. de genoemde tijden vraagt hij of deze zijn geschat indien de projecten gelijktijdig worden aangevat, dan wel als zij achtereenvolgens worden bekeken.

Heer de Fremery: "Min of meer gelijktijdig".

Prof.Oberman.....

GEHEIM

Prof. Oberman meent dat het wellicht niet noodzakelijk is direct al met het beste naar voren te komen; we zouden met een eenvoudige uitvoering kunnen beginnen, bv. als voorzetapparaat bij de ECOLEX IV. Ook zijn sleutelgenerator is als zodanig te bouwen. Deze is tevens zó geprojecteerd, dat het aantal wielen ad libitum kan worden uitgebreid. Hij meent dat we, uitgaande van deze eerste uitvoering door uitbouw met eenheden, tenslotte kunnen komen tot het beste. De klant kan dan door de keus te maken uit deze eenheden, zelf bepalen wat hem het meest geschikt lijkt. Evenwel moeten we het eerste eenvoudige apparaat cryptografisch sterk genoeg maken, anders zal het door de cryptologen zeker worden afgekeurd. Maw. we zullen ons moeten baseren op de internationale standaard voor cryptografische beveiliging, waaruit volgt dat de "ECOLEX V" een zeer sterke sleutelreeks moet kunnen genereren, daar de vercijfering in dit apparaat niet variabel is. Hij komt dan tot de volgende drie vragen:

1. is de eerste stap van USFA juist,
2. moet de daarin te verwerken sleutelgenerator al dié zijn, die ook gebruikt kan worden voor een verdergaand apparaat,
3. zijn er reeds voorstellen binnengekomen, die veilig genoeg zijn om bij de eerste stap te worden gebruikt?

Indien deze vragen bevestigend beantwoord kunnen worden, ziet hij de verdere ontwikkeling trapsgewijs. Op deze manier zouden we een kans hebben de concurrentie vóór te blijven. Als we nu echter beginnen met de ontwikkeling van het beste apparaat, zou deze wel eens zo lang kunnen duren, dat we te laat kwamen. Dit is het grote nadeel dat aan het voorstel van de Afd. B kleeft, nl. dat het veel tijd en veel geld vraagt om gerealiseerd te worden en misschien te star is voor de klant.
Verder meent Prof. Oberman dat gestreefd moet worden naar een tekstafhankelijke vercijfering, die ook uit eenheden is opgebouwd, zodat apparaten beschikbaar zullen komen zowel voor de lage classificaties alleen als voor de lage en hoge rubriceringen tezamen.

Prof. van Soest vindt de argumentatie van USFA een goede economische ondergrond hebben. Hij geeft een overzicht van de stand van zaken bij RVO-TNO. In het najaar komt het laboratorium-model gereed. Dan is in eerste instantie aan de ontvangen opdracht voldaan en is het aan de Minister van Defensie om te beslissen of verder gegaan zal worden. Zo ja, dan komen in de eerste helft van 1962 twee prototypes gereed. De CRYPTAUPHYL is ongeschikt om als bijzetapparaat te dienen bij de ECOLEX IV.

Heer de Fremery vindt de kleine efficiency in seinsnelheid van de CRYPTAUPHYL niet erg aantrekkelijk, nl. 64%.

Prof. van Soest antwoordt dat deze is op te voeren tot 92%, doch dan is de veiligheid van het systeem minder geworden.

Prof. Oberman meent dat de huidige apparatuur 100% efficiency eist en dat in de vercijfertechniek zélf de cryptografische veiligheid moet liggen. Verder acht hij het een groot bezwaar dat het uiterlijk van de cryptotekst van de CRYPTAUPHYL herkenbaar is, zodat uitsplitsing naar gebruikt systeem mogelijk wordt.

Prof. van Soest meent dat dit laatste niet zo'n groot bezwaar behoeft te zijn als het apparaat werkelijk goed is. "Nieuwe inzichten vereisen soms verandering van oude standpunten". Hij acht bv. het "at any time feature" van de CRYPTAUPHYL bijzonder aantrekkelijk.

De heer Luyt.....

De heer Luyt merkt nog op dat het uiterlijk van de cryptotekst gelijk is te maken aan een normale 32-tekst, door het bijloten van karakters weg te laten.

De voorzitter vraagt dan de vergadering wat nu de eerste stap moet zijn. Rekening houdend met de huidige mogelijkheden, is hij van mening dat het idee van USFA het beste is, dus een bijzetapparaat bij de ECOLEX IV. Daarnaast moet dan de verdere ontwikkeling ter hand worden genomen om tot een complete apparatuur te komen.

Heer Luyt constateert dat deze gang van zaken afwijkt van zijn advies, dat, indien dit direct ter hand wordt genomen, na een redelijke tijd een goed apparaat zal opleveren. Zijn bezwaar tegen het USFA voorstel is, dat er weer veel tijd verloren zal gaan bij het onderzoek naar een geschikte sleutelopwekker voor het bijzetapparaat. Zijn voorlopige indruk is, dat de sleutelontwikkeling van de Delftse Groep de voorkeur verdient om hiervoor deugdelijk te worden gemaakt.

De voorzitter oppert het idee om de regelmatige vervanging van de ECOLEX IV te wijzigen in een onregelmatige die in het bijzetapparaat zou moeten komen.

Heer Luyt zegt dat dit niet strikt nodig is als de sleutelgenerator cryptografisch sterk genoeg is.

Heer de Fremery stelt dat het oorspronkelijke voorstel van de Afd. B tenminste 1 jaar zal vergen tot de ontwikkeling van een prototype.

Prof. Oberman stelt deze tijd eveneens op 10 tot 14 maanden, doch dat geldt voor de ontwikkeling van een compleet apparaat zoals Afd. B het zou willen hebben. De ontwikkeling van een verbeterde sleutelgenerator volgens het principe van de Delftse Groep alleen, zal echter aanmerkelijk minder tijd kosten en niet meer dan de ontwikkeling van een verbeterde sleutelopwekking van het USFA-principe. Noodgedwongen is hij voor het voorstel van de voorzitter.

Nadat Prof. van Soest uiteen heeft gezet, dat RVO-TNO met zijn opdracht moet doorgaan tot de Minister over de verder te volgen weg met de CRYPTAUPHYL heeft beslist en van de voorzitter de toezegging heeft gekregen dat de aanbieding van dit apparaat aan de Standing Group(SECAN), los zal worden gezien van de oplossing die thans voorligt, verklaart hij zich voor het voorstel van de voorzitter.

De heer Luyt meent dat het voorstel de 2e prioriteit moet genieten.

Prof. Oberman stelt het volgende ontwikkelingsprogramma voor:

1. ECOLEX IV + sleutelopwekker,
2. id + id + tekstafhankelijke vercijfering,
3. id + id + id id + "foefjes", zoals automatische instelling e.d.

Heer Luyt .....

 GEHEIM

Heer Luyt stelt voor te beginnen bij 2 met een "Delftse" sleutel-generator.

Na een uitvoerige discussie wordt besloten tot het instellen van een sub-commissie, die in eerste instantie zal adviseren omtrent de keuze van het meest geschikte electronische "wiel" dat gebruikt zal worden bij de sleutelopwekking en verder zal zoeken naar een oplossing in de richting van een ECOLEX IV + sleutelgenerator + onregelmatige ver-vanging. RVO-TNO zal doorgaan met haar eigen project, rekening houdende met de kritieken die op de huidige CRYPTAUPHYL zijn binnengekomen.
RVO-TNO zal omstreks 1 september as. gereed hebben de onderliggende for-mule voor de sleutelopwekking, een beschrijving en het blokschema van het apparaat.
De Afd. B zal naar vermogen bijdragen de cryptografische waarde van de gewijzigde CRYPTAUPHYL te evalueren. Mede afhankelijk van dit onderzoek zal de NVBR dan kunnen beslissen of het apparaat dan aan de NATO zal worden aangeboden.
RVO-TNO blijft bereid om aan de verschillende commissies daadwerkelijk mede te werken.

de secretaris NVBR,

J.A. Versluis,
KLTZSD.