Stg. ZEER GEHEIM
Rubr.ambt.: secr. MR

Aantal pag.: 1
Aantal ex. : 30

MINISTERIELE COMMISSIE VOOR DE
INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Nr.15600a

Inhoudsopgave van
de vergadering van
4 juli 1995

Vdh/kvs
7/7/95

PERSOONLIJK cc:hr.v.d.Graaf

Nr.: 2014 3 juli 1995

Aan: De minister-president
Van: mr. J.P.M.H. Merckelbach

Betreft: Vergadering MICIV 4 juli 1995

U zou aan het begin van de vergadering de instemming van de MICIV kunnen vragen voor de aanwijzing van de heer G.L. Van den Hil, oud medewerker van de IDB en thans assistent van de coördinator van de inlichtingen- en veiligheidsdiensten, tot secretaris van de MICIV.

2. Cryptoproblematiek
De Covernota en de beslispuntennota zijn voorbesproken in een vergadering van het CVIN-plus op maandag 3 juli. De conclusies van deze vergadering zullen bij de aanvang van de MICIV-vergadering worden rondgedeeld.

Instemming van CVIN-plus en MICIV met de covernota en de beslispuntennota betekent:

a. Een gebundelde aanpak door de betrokken diensten van de cryptoproblematiek, met een ambitieniveau van 80% ontcijfering. De jaarlijkse kosten hiervan worden geraamd op ± 13 mln (14,5 minus 1,5 te hoog berekende personeelskosten) exogeen te financieren.

Zou de MICIV besluiten tot een gescheiden aanpak dan bedragen de extra jaarlijkse kosten 9 mln, te financieren binnen de betrokken begroting (8 mln Just en 1 mln BiZa). Dat lijkt aantrekkelijk, maar het is zeer de vraag of Just/BiZa zonder de expertise en de buitenlandse contacten van het TIVC, een ambitieniveau van 80% kunnen bereiken resp. lange tijd kunnen handhaven.

b. Dat het CVIN zal optreden als scheidsrechter bij geschillen over het gebruik van ontcijferde informatie in de rechtzaal. Daarbij is intern in het CVIN afgesproken dat uiteindelijk elk lid een recht van veto heeft.

c. Dat nadere evaluatie's/studies dienen te worden verricht m.b.t.
- een periodieke evaluatie van het voorgestelde samenwerkingsverband; m.i. in het CVIN-MICIV circuit.
- de overeenkomst tussen de Staat en Philips Crypto ook t.a.v. de offensieve aanpak, onder auspiciën van het CVIN.
- wettelijke maatregelen in het kader van de offensieve cryptoproblematiek; voor te bereiden door de werkgroep Patijn (Just), na afloop van de parlementaire enquête o.l.v. Van Traa.

Me/kvs

micIV. Archief
micIV 04-07-1995
punt 1b.

Stg. ZEER GEHEIM
Rubr.ambt.: secr MR

Aantal pag.: ~~79~~
Aantal ex. : 30

MINISTERIëLE COMMISSIE VOOR DE INLICHTINGEN
EN VEILIGHEIDSDIENSTEN

Nr.15408

Ex.nr. 53

Notulen van de vergadering gehouden op
dinsdag 24 januari 1995 in de Trêveszaal
van het Kabinet van de Minister-President,
's morgens van 09.00-10.30 uur

Aanwezig: minister-president Kok en de ministers Dijkstal, Sorgdrager, Voorhoeve en Zalm.

Voorts zijn aanwezig: mevrouw Plesch (wnd. SG BiZa) en de heren Kok (hfd. MID), Kievits (wnd. hfd. BVD), Meulmeester (AZ), Engering (DG-BEB, EZ), Hendriks (plv. SG Fin), Van Brummen (DG-PC, Just), Van Eenennaam (plv. DGPZ, BZ) en Barth (wnd. SG-Def).

Secretaris en wnd. Coördinator IenV: Mr. J.P.M.H. Merckelbach.
Adjunct-secretaris: Ir. D.K.A.M. Minten.

1. Notulen van de vergadering van 23 februari 1993 (nr. 14679)

Ongewijzigd vastgesteld.

2. Mededelingen
(nr. 95G000006, d.d. 20 januari 1995)

Minister Dijkstal geeft aan twee mededelingen te willen doen. Ten eerste betreft dat de plaatsing van een BVD-liaison te Singapore. Deze permanente liaison zal de Zuid-Oost Aziatische regio bestrijken. De keuze

is niet op Bangkok gevallen, o.a. omdat daar reeds een CRI-liaison is gevestigd en spreker het verstandig acht de liaisons over de regio te spreiden. Uiteraard zullen zij onderling contacten onderhouden. De tweede opmerking betreft de klachten over de unie van Marokkaanse Moslim-organisaties in Nederland (UMMON) betreffende de ongepaste wijze waarop deze organisatie zich met in Nederland wonende Marokkanen bemoeit. Bij nader onderzoek is terzake niet veel concreet bewijsmateriaal aangetroffen. Echter de zorgen over mogelijke intimidatie blijven bestaan. In de komende weken zal de vaste commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer vertrouwelijk worden geïnformeerd over de situatie m.b.t. intimidatie van in Nederland wonende minderheden en in Nederland verblijvende asielzoekers. Spreker is voornemens deze commissie dan ook in te lichten over de UMMON.

De Commissie stemt vervolgens in met de plaatsing van een BVD-liaison te Singapore. De minister van Binnenlandse Zaken zal de vaste commissie voor de inlichtingen- en veiligheidsdiensten informeren over de situatie met betrekking tot intimidatie van in Nederland wonende minderheden alsmede in Nederland verblijvende asielzoekers.

3. Versterking functie MICIV
(nr. 95G000007, d.d. 20 januari 1995)

Minister Dijkstal geeft een korte toelichting op de voorliggende notitie van de BVD. Ten eerste is hem gebleken dat er vanuit bestuurlijk en ambtelijk oogpunt voldoende onderwerpen voorhanden zijn om meerdere malen per jaar overleg te hebben. Voorts hebben de drie coalitie partijen in de afgelopen jaren duidelijk een standpunt ingenomen betreffende de manier waarop de veiligheidsdiensten gecontroleerd zouden moeten worden alsmede dat het parlement een sterkere rol zou moeten worden toegekend. Spreker is bereid zijn oorspronkelijke standpunt enigszins te nuanceren als de MICIV maar met een hogere frequentie zal gaan vergaderen om zo een adequate politieke controle op de diensten te kunnen uitoefenen.

De minister-president kan ermee instemmen de intensiteit en de frequentie van het overleg in de MICIV te verhogen en de inhoud van het overleg te verbreden. Hij stelt voor om daarbij onderscheid te maken tussen operationele kwesties, waarbij een goede communicatie tussen meer direkt betrokken bewindspersonen van belang

is en een bredere taakuitoefening van de MICIV. Hij vraagt zich af wat de instemming van de MICIV met de voorliggende notitie in feite zal betekenen. De MICIV zal dan in beginsel zeker drie keer per jaar bijeenkomen: in beperkte samenstelling indien er alleen over de operationele aspecten van de diensten gesproken wordt en in brede samenstelling als er algemene beleidsmatige thema's aan de orde zijn.

Minister Zalm heeft er geen bezwaar tegen indien Financiën niet meer bij het verdere overleg in het kader van de MICIV betrokken zou worden. Over financiële zaken kan ook bilateraal overleg worden gevoerd.

Minister Sorgdrager merkt op dat de frequentie van het overleg ook verband houdt met de visie op de rol van de MICIV en de onderwerpen die in de MICIV besproken behoren te worden. Eén vergadering per jaar kan bijna niet meer zijn dan een formaliteit; zo kan de MICIV geen reële betekenis hebben. Alleen vaker vergaderen geeft mogelijkheden voor een nauwere betrokkenheid bij de inlichtingen en veiligheidsdiensten. Zij geeft daar de voorkeur aan, ook vanwege de vele raakvlakken tussen het werk van de diensten en de bestrijding van de georganiseerde criminaliteit.

De heer Engering stemt met het voorstel in. Vanuit Economische Zaken bestaat de behoefte om betrokken te blijven in verband met non-proliferatie en zaken zoals de cryptografie. Economische Zaken hoeft niet betrokken te worden bij overleg over de operationele aspecten van de diensten.

Minister Voorhoeve sluit zich bij de vorige sprekers aan mede in het licht van de problemen m.b.t. tot de Nederlandse-Antillen en Aruba.

De minister-president concludeert dat de MICIV in beginsel drie maal per jaar zal vergaderen, in januari, in april en in oktober. Wanneer uitsluitend de operationele aspecten van de diensten aan de orde komen behoeven de ministers van Financiën en Economische Zaken niet aan de vergadering deel te nemen.

De Commissie stemt hiermee in.

4. De functie van coördinator van de inlichtingen- en veiligheidsdiensten
(nr. 95G000004, d.d. 20 januari 1995)

Minister Dijkstal heeft vernomen dat in het verleden de secretaris-generaal van Algemene Zaken tevens coördinator was van de inlichtingen- en veiligheidsdiensten. Hij vraagt waarom daar thans in het voorliggende voorstel van wordt afgeweken.

De minister-president antwoordt dat de huidige secretaris-generaal van Algemene Zaken zich tot nu toe niet met het beleidsterrein van de inlichtingen- en veiligheidsdiensten heeft beziggehouden en daarom een omschakeling zal moeten maken om zich op dit gebied in te werken terwijl de wnd. coördinator, de heer Merckelbach, volledig in de materie is ingevoerd. Er is een pragmatische afweging gemaakt, betreffende de wijze waarop in deze optimaal van de beschikbare kwaliteiten en ervaringen gebruik zou kunnen worden gemaakt. Om deze reden is gekozen voor de voorliggende voordracht ter benoeming.

De Commissie stemt vervolgens in met de voordracht tot benoeming van
mr. J.P.M.H. Merckelbach tot coördinator I&V.

5. Presentatie over de crypto-problematiek
(nr. 95G000008. d.d. 20 januari 1995)
(MICIV 23 februari 1993, punt 4)

Minister Voorhoeve onderstreept naar aanleiding van de presentatie van de heer Kok inzake de crypto-problematiek, het grote belang van dit onderwerp vooral met het oog op de groei van de internationale criminaliteit. Het Technisch Informatie- en Verbindingscentrum (TIVC) onderschept in toenemende mate berichten die van nut zijn voor de bestrijding van de criminaliteit. Daarom is de groeiende samenwerking tussen de diensten van belang.

Minister Sorgdrager geeft aan dat naast de crypto-problematiek ook de aftapbaarheid van telecommunicatie in toenemende mate een probleem wordt. Aan de aanbodzijde is thans alleen nog maar de PTT op de markt, maar er komen spoedig nieuwe aanbieders. Dan zal moeten worden bezien op welke wijze deze nieuwe systemen aftapbaar kunnen worden gemaakt en wie de kosten van een dergelijke operatie zal dragen. Het aftappen van telecommunicatie is van groot belang bij het opsporen van misdrijven. In Nederland ligt de verhouding tussen het aantal aftappingen

en het aantal daardoor opgeloste misdrijven wel anders dan in de Verenigde Staten. Aftappen blijft echter een onmisbaar hulpmiddel.
Spreekster vraagt zich af of het mogelijk zal zijn met een wettelijke regeling overheidsonvriendelijke cryptografie tegen te gaan. In het reguliere verkeer zal deze wetgeving wel handhaafbaar zijn maar t.a.v. het criminele verkeer zal de situatie veel moeilijker liggen.

Minister Dijkstal onderscheidt een aantal aspecten. In de eerste plaats de vraag wat de wettelijke mogelijkheden zijn om in systemen in te breken. Ten tweede gaat het om de fysieke mogelijkheden om in te breken en af te tappen. Vervolgens moet de afgetapte informatie in crypto kunnen worden gelezen en tenslotte is er de vraag of de geanalyseerde informatie bij het opsporingsonderzoek kan worden gebruikt. Deze aspecten beïnvloeden elkaar en moeten in hun onderlinge samenhang worden bezien, juridisch, organisatorisch en financieel.
Het is spreker nog niet duidelijk wat met offensief en defensief wordt bedoeld ook in relatie met de informatiebeveiliging. Hij zou een en ander nader uitgewerkt willen zien evenals de vraag in hoeverre de inspanningen op cryptogebied andere inspanningen kunnen vervangen. Het volgen van een verdachte is bijvoorbeeld niet nodig als men via aftappen en de computer ook aan de benodigde informatie kan komen. Voorts wijst hij op het rapport van het Beleidsadviescollege Politiële Informatievoorziening onder voorzitterschap van de heer Hermans over de politiële informatie-ontwikkeling in de toekomst en de beveiliging daarvan. Nagegaan zal moeten worden welke raakvlakken dat rapport heeft met de materie die thans aan de orde is. Op basis van het rapport van de commissie Hermans wordt voorgesteld f. 400 mln. extra uit te trekken voor automatisering op rijks- en regionaal niveau. Indien deze financiële middelen al zouden kunnen worden vrijgemaakt, zal moeten worden bezien of deze op onderdelen mede ten nutte van de oplossing van de crypto-problematiek kunnen worden aangewend.

Minister Zalm spreekt zijn waardering uit over de presentatie die in onderlinge samenwerking tussen de diensten tot stand is gekomen. Hij constateert dat de beschikbare capaciteit gerelateerd aan de behoefte nogal scheef over de diensten is verdeeld: de BVD beschikt over een minimale capaciteit, Justitite over een geringe, maar Defensie heeft een enorme capaciteit. In de schets van de toekomstige ontwikkelingen werd aangegeven dat de grootste

problemen op het gebied van justitie te verwachten zijn en niet op dat van defensie. Hij betwijfelt of de huidige capaciteitsverdeling daarbij voldoende aansluit, zeker wanneer Justitie slechts incidenteel door Defensie wordt geholpen. Het gaat hier dus om de keuze van de goede prioriteiten. Tenslotte vraagt spreker of de betrokken collega's al onderling overleg hebben gevoerd over de omvang van extra uitgaven en de dekking daarvan.

De heer Engering constateert dat de explosieve toename in het gebruik van cryptografie vooral binnen het bedrijfsleven plaatsvindt. De vraag is hoe de voor de Staat relevante informatie die onderschept en ontcijfert moet worden kan worden onderscheiden van de grote stroom versluierd berichtenverkeer binnen het bedrijfsleven die voor de overheid niet relevant is. Stel dat 90% van de cryptografie voor de overheid niet relevant is dan moet de overheid toch niet proberen alles te analyseren.

De minister-president vraagt, naar aanleiding van het begrip "overheidsvriendelijk" of nog eens precies gedefinieerd kan worden wat vanuit het algemeen belang de grenzen zijn van de toelaatbaarheid en noodzakelijkheid van offensief optreden in deze. Met betrekking tot de aangegeven achterstand op het gebied van de cryptografie vraagt hij of voor 1990 ook al sprake was van een achterstand. Een volgende vraag is of de achterstand die met het handhaven van de bestaande activiteiten tussen 1995 en 2000 zou worden opgelopen een vaststaand of een arbitrair gegeven is vanwege ondermeer de ontwikkeling van nieuwe technieken.
Spreker vraagt voorts in hoeverre gebruik wordt gemaakt van internationale samenwerking met betrekking tot het gezamenlijk ontwikkelen en hanteren van technieken of infrastructuren op het militaire vlak of op dat van de grensoverschrijdende criminaliteit. Evenals minister Dijkstal vraagt spreker zich af of andere actviteiten op een lager pitje kunnen worden gezet als het crypto-plan wordt uitgevoerd. Tenslotte zit spreker met de vraag hoe ons ambitieniveau zal worden bepaald; wat is de graadmeter voor de afweging tussen inspanning en voldoende resultaat.

De heer Kok antwoordt in reactie op de vragen van de minister-president en minister Zalm dat het onderscheppen en kraken van versluierde berichten veruit het grootste aandeel oplevert - 75 à 85% - van alle inlichtingen. De onderschepte berichten zijn niet altijd voor

Nederland relevant, maar kunnen van belang zijn voor de bondgenoten. De uitruil van deze informatie kan informatie opleveren die wel direct van belang is voor Nederland. De informatie uit open bronnen en uit human intelligence is qua omvang bijna te verwaarlozen tegenover de informatie uit verbindingsinlichtingen.

Minister Dijkstal vraagt of daaruit kan worden geconcludeerd dat niet gerichte activiteiten af en toe resultaten kunnen opleveren.

De heer Kok antwoordt dat er toch sprake is van gerichte activiteiten. Er wordt gewerkt aan de hand van een nationale wensenlijst die ook via samenwerking en uitruil met de partners wordt ingevuld.

De minister-president was wel op de hoogte van het bestaan van deze "postzegelbeurs", maar zijn vraag had meer betrekking op internationale samenwerking bij het ontwikkelen van de kostbare infrastructuur.

De heer Kok antwoordt dat een dergelijke samenwerking ook plaatsvindt vooral op bilaterale basis. Zo worden de "kastjes" ontwikkeld die crypto-systemen kunnen kraken. Dat is een kostbare activiteit waarbij ook het resultaat gezamenlijk wordt geexploiteerd. Dat leidt ook tot een veel grotere analysecapaciteit in het vervolgtraject. Spreker noemt ter illustratie dat men in de bekende RaRa-zaak stuitte op vercijferde bestanden, die het gerechtelijk laboratorium en ook het TIVC niet kon analyseren. De bestanden zijn toen naar de Verenigde Staten gezonden waar men ook maar een klein gedeelte heeft kunnen ontcijferen. De gepresenteerde prognose over de omvang van de cryptoproblematiek is deels gebaseerd op deskundigheid en deels op het extrapoleren van gegevens uit de voorgaande jaren. De prognose die in het voorjaar van 1993 is gemaakt blijkt na twaalf maanden nog aardig te kloppen.

De heer Van Brummen gaat naar aanleiding van de opmerking van de minister-president nader in op het ambitieniveau en de succesmogelijkheden. Bij het gerechtelijke laboratorium - de afdeling forensisch computeronderzoek - is gebleken dat het aantal analyse-verzoeken is toegenomen van 58 in 1992 tot 135 in 1995. In deze tijd is het aantal formatieplaatsen van 1 tot 5 toegenomen. Aan 80% van de verzoeken kan worden voldaan. Daaruit blijkt dat de genoemde afdeling in staat is om tot een redelijke successcore te komen. De balansverschuiving van Defensie naar Justitie heeft te maken met het feit dat het hanteren van cryptografie explosief toeneemt in de criminele

sfeer. Daarom zijn juist bij de BVD en Justitie snelle investeringen nodig.

De heer Kievits meent dat een aantal van de gestelde vragen vanuit de MICIV kan worden uitbesteed aan het CVIN ter voorbereiding van besluitvorming in de voorjaarsvergadering van de MICIV. Van de technische middelen in het kader van de cryptografie maakt de BVD minder gebruik dan de andere diensten. Toch acht hij de genoemde technieken onmisbaar en steunt hij het voorstel tot intensivering van de cryptoactiviteiten. Het blijft echter een beperkt hulpmiddel; goed opgeleide spionnen houden rekening met het kraken van crypto. Ook de internationale samenwerking kent zijn beperkingen, zoals blijkt in de RaRa-zaak, maar dient toch maximaal te worden benut. De BVD richt zich met name op de fasen voor en na het hanteren van cryptografie. Dat is een andere manier om informatie te verkrijgen. Het gaat niet alleen om de technische maar ook om de operationale aspecten.

De heer Meulmeester onderschrijft de opmerking dat er sprake is van zowel technische als operationele aspecten. Welke berichten ook worden onderschept altijd zal moeten worden bezien wat de intentie van de verzender is en of de ontvanger het bericht ook zo zal willen uitvoeren. De techniek is belangrijk maar het gewone handwerk blijft onmisbaar. Cryptografie is zo belangrijk geworden dat bepaalde bondgenoten teams over de wereld sturen die trachten cruciale apparatuur in bezit te krijgen om bepaalde berichtgeving te kunnen ontcijferen. Datzelfde geldt ook voor criminele organisaties die veel geld en professionele deskundigheid tot hun beschikking hebben en veel verder zullen gaan dan het stelen van floppies met geheime informatie.

Minister Voorhoeve sluit zich hierbij aan. Ook uit de discussie blijkt dat verbindingsinlichtingen van groeiend belang zijn voor de rechtshandhaving en de staatsveiligheid en een steeds belangrijker bijprodukt van de militaire inlichtingendiensten. Om de taken goed te kunnen uitvoeren is een extra inspanning nodig van f. 25 mln. per jaar. Defensie kan deze financiële middelen echter niet verschaffen. Het betreft een investering in het algemeen belang en binnen de begroting van Defensie is hiervoor geen ruimte. Buitenlandse Zaken, Justitie, Binnenlandse Zaken, Algemene Zaken en Defensie hebben hier een gezamenlijk probleem van f. 100 mln. in de komende vier jaar, willen wij niet op een onoverbrugbare achterstand komen.

De heer Kok merkt op dat er een

fundamenteel verschil bestaat tussen de benadering van Justitie en de inlichtingen- en veiligheidsdiensten. Justitie is reactief; het reageert op feiten die zich hebben voorgedaan en is uit op het verkrijgen van bewijzen. De inlichtingen- en veiligheidsdiensten zijn pro-actief en brengen de risico's in kaart waartegen nog maatregelen genomen kunnen worden, waarbij men minder geënteresseerd is in het verkrijgen van bewijzen.

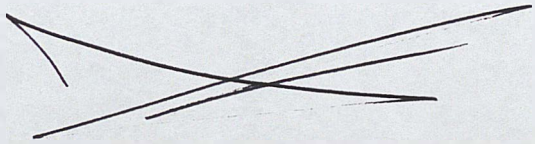
Minister Dijkstal wijst erop dat politie en justitie zich ook steeds meer pro-actief opstellen. Criminaliteitsbestrijding heeft in toenemende mate te maken met de staatsveiligheid en komt daarmee op het aandachtsterrein van de BVD. Ter illustratie noemt hij het BVD-onderzoek naar de betrokkenheid van militairen bij de drugshandel in Suriname. Langzamerhand zijn er veel departementen met gelijke belangen bij dit soort onderzoek betrokken.

De heer Kok wijst op het feit dat buitenlandse partners van de diensten terughoudend zijn met het verstrekken van informatie als zij weten dat deze ook wordt gebruikt in de rechtzaal.

De minister-president stelt de volgende conclusies voor:
Het CVIN zal, gehoord het besprokene in de commissie, een beslispuntennota t.b.v. de MICIV-vergadering in april 1995 voorbereiden.*

Hierbij zal als leidend beginsel worden gehanteerd een gebundelde aanpak en een optimale benutting van de beschikbare capaciteit van alle betrokken diensten. Voorts zal de nota een helder, ook voor de Kamer bruikbaar, beeld moeten schetsen van de crypto-problematiek.

De Secretaris,



* De Ministerraad heeft in zijn vergadering van 27 januari 1995 (agendapunt 12) besloten dat ook VW en EZ bij de voorbereiding van deze nota zullen worden betrokken.

0018D-67
Me/kvs
1 februari 1995

rel. punt 2

Stg. Confidentieel

nr. 95G000069
22-6-1995

Ter voldoening aan de opdracht van de MICIV van 24 januari 1995 wordt u hierbij aangeboden een beslispuntennota met betrekking tot de operationele cryptoproblematiek.
Deze nota wordt voorafgegaan door een "covernota" waarin een inzicht wordt gegeven in de wijze waarop de beslispuntennota tot stand is gekomen en welke punten van overweging daarbij een rol hebben gespeeld, c.q. welke onderwerpen nog nader dienen te worden beschouwd.

A. COVERNOTA

1. Op 24.1.1995 besloot de MICIV dat het CVIN een beslispuntennota over de cryptoproblematiek diende op te stellen ter bespreking in een volgende MICIV.
Het CVIN stelde vervolgens de "Werkgroep Cryptografie" in onder voorzitterschap van drs. K.M. Meulmeester. Deze werkgroep kreeg de opdracht een beslispuntennota inzake de cryptoproblematiek voor te bereiden met als uitgangspunten een gezamenlijke aanpak van de betrokken diensten en een optimale benutting van de bij die diensten aanwezige capaciteit. Tevens werd aan de werkgroep een aantal vragen gesteld, ontleend aan de in de MICIV gevoerde discussie.
De thans voorliggende beslispuntennota is het resultaat waartoe de werkgroep, met terugkoppeling naar het CVIN, gekomen is.
Het CVIN oordeelt het van belang om ten aanzien van de totstandkoming en de betekenis van deze nota nog de navolgende kanttekeningen te plaatsen:

a. In opdracht van het CVIN heeft de werkgroep zich met name gericht op de praktische aanpak van de operationele cryptoproblematiek. Dit is slechts een onderdeel is van een veelomvattender vooral juridisch probleemveld maar kan daarvan niet los worden gezien.

b. Daar de eerste vergaderingen van de Werkgroep Cryptografie vooral op de operationeel-technisch samenwerking tussen de betrokken diensten gericht waren zijn de vertegenwoordigers van de ministeries van Economische Zaken en Verkeer en Waterstaat eerst in een later stadium uitgenodigd de vergaderingen bij te wonen.

c. Alhoewel het tot de opdracht van de werkgroep behoorde uit te gaan van een gezamenlijke aanpak en een optimale benutting van de aanwezige capaciteit van de betrokken diensten is, op uitdrukkelijke wens van het ministerie van Defensie, de huidige capaciteit van het TIVC buiten beschouwing gelaten. Voor Defensie is een herverdeling en herbezetting van die capaciteit geen bespreekbare optie. Overigens acht ook het CVIN het niet mogelijk om alle problemen met de nu ter beschikking staande mensen en middelen op te lossen.

Voor Biza (BVD) en Justitie (DGPC) bestond en bestaat nog steeds een alternatief voor de in bijgaande beslispuntennota omschreven gezamenlijke operationele aanpak van de cryptoproblematiek. Deze departementen kunnen, indien de MICIV zulks zou prefereren, los van het TIVC, zelfstandig een bilateraal samenwerkingsverband opzetten voor de operationele aanpak van de cryptoproblemen waarmee zij worden geconfronteerd. Een dergelijk samenwerkingsverband zou een jaarlijkse investering van circa fl. 9 miljoen vergen (Justitie: fl 8 miljoen, Biza: fl 1 miljoen).
De werkgroep is, na tussentijdse terugkoppeling met het CVIN, tenslotte tot de conclusie gekomen dat de door de MICIV gewenste en in bijgaand verslag omschreven samenwerking van alle betrokken diensten de voorkeur verdient boven een gescheiden optrekken. De meerwaarde van een gezamenlijke aanpak is niet alleen een efficiënter gebruik van de schaarse capaciteit aan hoogwaardige mensen en de relatief kostbare infrastructuur. Ook voor het gebruik van externe expertise en capaciteit ontstaan, door het TIVC in de samenwerking te betrekken, veel meer mogelijkheden. Het CVIN verwacht dat, ook indien aanvankelijk gekozen zou worden voor een gescheiden aanpak, uiteindelijk toch een samenwerkingsverband van alle betrokken diensten noodzakelijk zal blijken.

d. Het was de wens van het CVIN om in (een bijlage bij) deze beslispuntennota (zie punt I.4, onder D. 1e, en beslispunt II.3) objectieve criteria te kunnen aangeven op grond waarvan beslissingen over de exploitatie van ontsluierde cryptogegevens ter terechtzitting kunnen worden genomen. Bij het overleg over deze criteria zijn de betrokken diensten gestoten op een aantal zowel technische als juridische gecompliceerde problemen. Daarom blijkt dit overleg meer tijd te vergen dan aanvankelijk voorzien was. Het laat zich aanzien dat eerst met succes dergelijke criteria kunnen worden geformuleerd indien de werkzaamheden van de parlementaire enquetecommissie onder voorzitterschap van het Tweede Kamerlid Van Tra zijn beëindigd. Te verwachten valt dat de enquetecommissie ten aanzien van crypto-gerelateerde zaken aanbevelingen zal doen.

e. De hieronder genoemde vraagpunten die de leden van de MICIV hebben opgebracht worden niet afzonderlijk in het verslag van de werkgroep behandeld.

<u>Toelichting</u>

-De vraag of opsporingsactiviteiten kunnen worden afgestoten indien een intensiever gebruik wordt gemaakt van cryptotechnieken moet ontkennend worden beantwoord. Een reeds bestaande achterstand op cryptogebied dient ingehaald te worden; alleen daarom is al een extra inspanning noodzakelijk. De andere methoden die bij het vergaren van inlichtingen en opsporingsgegevens gebruikt worden zijn complementair en kunnen moeilijk worden gemist. Wel is het te verwachten dat Justitie door het gebruik van cryptotechnieken veel

rel. punt 2

Stg. Confidentieel

nr. 95G000070
22-6-1995

B. BESLISPUNTENNOTA

I. INLEIDING

I.1

Cryptografie ofwel geheimschrift is het versluieren van informatie via een geheime sleutel. Van oudsher wordt cryptografie gebruikt door de ministeries van Defensie en Buitenlandse Zaken. Door de snelle ontwikkelingen op het gebied van telecommunicatie en computertechnologie doet de cryptografie nu op grote schaal zijn intrede op de zakelijke- en consumentenmarkt. Kort samengevat is dit de kern van enerzijds het economisch-maatschappelijk belang van cryptografie en anderzijds de cryptoproblematiek waarmee opsporingsdiensten en inlichtingen- en veiligheidsdiensten geconfronteerd worden doordat zij in toenemende mate belangrijke inlichtingen over bijvoorbeeld criminele organisaties moeten ontberen.
De cryptoproblematiek wordt gecompliceerd door de verschillende belangen van de betrokken overheidsdiensten.
De MICIV heeft opdracht gegeven oplossingen te zoeken waarbij een gezamenlijke aanpak/optimale benutting van de aanwezige capaciteit als uitgangspunt geldt.
Deze nota is overwegend toegespitst op de operationele aanpak van de cryptoproblematiek middels een praktisch gerichte invalshoek. De operationele aanpak is echter slechts een onderdeel van het totale probleemveld inzake cryptografie.

De totale problematiek omvat een zestal onderwerpen, te weten:

* het nemen van wettelijke maatregelen (de Werkgroep Patijn doet hiertoe voorstellen);
* het ontwikkelen van overheidsvriendelijke crypto ;
* instandhouding van de nationale crypto-industrie (overeenkomst Staat-Philips Crypto n.a.v. standpunt MICIV van maart 1993);
* het crypto-exportbeleid;
* de nationale en internationale afstemming;
* de operationele aanpak.

I.2

De cryptoproblematiek is aan de orde bij de verwerving van:

a) militaire inlichtingen en strategische inlichtingen;
b) inlichtingen ten behoeve van Justitie, Politie en de BVD.

bewijsmateriaal op eenvoudiger wijze en met minder risico's kan vergaren.

-Met betrekking tot de vraag of er raakvlakken bestaan tussen de conclusies van het Beleidsadviescollege voor de Politiële Informatievoorziening (BPI ofwel de "Commissie Hermans") en de hier aan de orde zijnde cryptoproblematiek en met name de vraag of eventueel financiële middelen voor politiële informatievoorziening mede ten nutte van de oplossing van de cryptoproblematiek kunnen worden aangewend luidt de conclusie dat er alleen raakvlakken zijn ten aanzien van de toepassing van defensieve cryptosystemen ten behoeve van politie-communicatiemiddelen. Het NBV speelt hierbij een belangrijke rol. Dit levert vooralsnog echter geen additionele mogelijkheden tot financiering op.
In hoeverre uit het Project zware georganiseerde criminaliteit financiële middelen kunnen worden vrijgemaakt ten behoeve van de additionele cryptoproblematiek kon de werkgroep niet overzien, omdat dit een zaak wordt van interne herschikking.

De operationele aanpak betreft de onder b) genoemde "inlichtingen ten behoeve van Justitie, Politie en de BVD". De onder a) genoemde inlichtingen zijn van oudsher - met name bij Defensie, BZ en BVD - bestaande behoeftes aan militaire en strategische verbindingsinlichtingen. De verwerving en produktie hiervan is ondergebracht bij het Technisch Informatieverwerkingscentrum (TIVC) van het ministerie van Defensie en staat los van de verwerving van inlichtingen zoals genoemd onder b) ten behoeve van Justitie, Politie en BVD. De cryptoproblematiek bij de verwerving van inlichtingen ten behoeve van Justitie, Politie, de Fiod en BVD bestaat nog maar kort. De problemen worden veroorzaakt doordat nu, in tegenstelling tot vroeger, een ieder eenvoudiger kan beschikken over middelen om informatie te versluieren. Deze nieuwe problemen vragen om een snelle en adequate oplossing aangezien opsporingsinstanties - vanwege de termijnen die worden voorgeschreven in het Wetboek van Strafvordering - veelal onder tijdsdruk moeten werken. Op het Gerechtelijk Laboratorium (GL) van het ministerie van Justitie is deskundigheid aanwezig om met name het Openbaar Ministerie, de Politie en de bijzondere opsporingsdiensten te ondersteunen bij het toegankelijk maken van versluierde informatie. Echter, gelet op de sterke groei en complexiteit van de problemen is een nationale geïntegreerde aanpak bestaande uit een nauwe samenwerking tussen het GL, de BVD, het Nationaal Bureau voor Verbindingsbeveiliging (NBV) en het TIVC nodig om de reeds opgelopen achterstand in te lopen en het hoofd te kunnen bieden aan de problemen die nu op ons af komen. De actuele problemen op het gebied van de operationele aanpak van de cryptoproblematiek zijn niet op te lossen met het huidige personeelsbestand en capaciteit in de bestaande organisatiestructuur van de diverse diensten. Ook een herverdeling en herbezetting van capaciteit zal niet tot voldoende resultaat leiden en is voor het ministerie van Defensie geen optie.

I.3

De navolgende definities worden gehanteerd.

<u>offensieve crypto:</u> het breken van cryptografische systemen (crypto-analyse);

<u>defensieve crypto:</u> het gebruik van cryptografie om informatie te versluieren voor derden.

Ten aanzien van de offensieve crypto zijn het TIVC en het GL de uitvoerende organisaties. Zij verrichten hun werkzaamheden voor uiteenlopende ministeries en/of diensten, namelijk Defensie, Justitie, Buitenlandse Zaken, de BVD, het Openbaar Ministerie (OM), de Politie en bijzondere opsporingsinstanties.

Het NBV is verantwoordelijk voor de bijzondere informatiebeveiliging op het gebied van de defensieve crypto en adviseert terzake de cryptografische informatiebeveiliging ten behoeve van de gehele rijksoverheid.
Offensieve en defensieve cryptografie zijn nauw met elkaar verwant: er wordt gebruik gemaakt van dezelfde expertise, zij het vanuit een andere invalshoek. Op het uitvoerend niveau wordt een zeer strikte scheiding doorgevoerd op basis van het "need to know"-principe, waarbij expliciet gesteld wordt dat de defensieve component geen operationele crypto-analyse uitvoert, terwijl de offensieve component geen keuringen zal uitvoeren. Voor zover niet strijdig met de taak, houdt het NBV reeds lang rekening met de belangen van het TIVC.

I.4

De voornaamste conclusies van de Werkgroep Cryptografie zijn:

A. Een gebundelde aanpak leidt tot efficiëntiewinst doordat de aanwezige capaciteit optimaal benut wordt, echter, een optimale benutting van de aanwezige capaciteit is onvoldoende om de huidige problematiek op te lossen.

B. Het opsporings- en het staatsveiligheidsbelang vereisen dat circa 80% van de aangeboden versluierde berichten door middel van ontcijfering tijdig leesbaar kan worden gemaakt. Geschat wordt dat dit percentage overeenkomt met een noodzakelijk extra budget van circa fl. 14,5 miljoen per jaar (zie bijlage).

C. De voorgestelde operationele aanpak is een deeloplossing van het totale probleemveld inzake cryptografie.

D. Aandacht dient te worden besteed aan de volgende punten:

   1e. De exploitatieproblematiek dient nader uitgewerkt te worden. Hierbij dienen de opsporings-, de staatsveiligheids- en de internationale veiligheidsbelangen te worden afgewogen.

   2e. Een periodieke evaluatie van de toegevoegde waarde van het voorgestelde samenwerkingsverband in relatie tot het kostenniveau is gewenst.

II. **BESLISPUNTEN**

II.1.

De overeenkomst tussen de Staat en Philips Crypto dient ook in relatie tot de operationele aanpak van de cryptoproblematiek te worden geëvalueerd.

Toelichting:

Het belang van de nationale crypto-industrie is o.m. dat de overheid autonoom tot op het hoogste beveiligingsniveau in de eigen behoefte kan voorzien. Die activiteit draagt bij aan een hoog niveau van inhoudelijke cryptografische expertise bij de overheid zelf en speelt een rol in de contacten en uitwisseling van gegevens met bondgenoten in een overeenkomstige situatie hetgeen ook de operationele belangen ten goede komt.

II.2.

Het nemen van wettelijke maatregelen in het kader van offensieve cryptoproblematiek is een vereiste.

Toelichting:

De grenzen van de toelaatbaarheid en noodzakelijkheid van offensief optreden moeten zodanig zijn dat voorkoming of effectieve opsporing van criminele en terroristische activiteiten mogelijk blijft. Ten aanzien van de toelaatbaarheid ziet de Werkgroep geen wettelijke beperkingen. Zonder vooruit te willen lopen op de voorstellen van de Werkgroep Patijn zouden de volgende in die Werkgroep voorgestelde alternatieven, gezien vanuit een technisch perspectief, de kansen op succes van de operationele aanpak kunnen verhogen:

1. De verplichting voor aanbieders van telecommunicatie-infrastructuren en -diensten om het oorspronkelijk signaal aan te leveren.
2. De instelling van een verplichting tot medewerking ten behoeve van (opsporings-)onderzoek voor gebruikers van cryptografie.
3. Een verplichting tot registratie van cryptografie die commercieel wordt aangeboden.
4. De mogelijkheid scheppen het gebruik van cryptografie incidenteel te verbieden.

II.3.

Het CVIN wordt belast met beslissingsbevoegdheid ten aanzien van vraagstukken van exploitatie die niet middels objectieve criteria kunnen worden beantwoord.

Toelichting:

Met betrekking tot exploitatie van gegevens (het gebruik van ontcijferde informatie in de rechtszaal) is geregeld werkoverleg tussen de betrokken diensten noodzakelijk en mogelijk. Daar waar knelpunten in de exploitatie van cryptogegevens optreden zal het CVIN deze dienen op te lossen. Hierbij beoordeelt het CVIN het vraagstuk mede op grond van het opsporingsbelang, het staatsveiligheidsbelang en het internationale veiligheidsbelang.
Verwacht mag worden dat zich in de praktijk slechts in beperkte mate problemen zullen voordoen ten aanzien van de exploitatie. Hiertoe dienen objectieve criteria nader te worden geformuleerd en uitgewerkt. Het formuleren van deze criteria zal naar verwachting geen problemen opleveren bij de uitwerking van de geïntegreerde operationele aanpak.
Ten aanzien van het mogelijke probleem van de contra-expertise wordt het volgende opgemerkt.
De raadsman van verdachte(n) kan ter terechtzitting vraagtekens plaatsen bij de wijze waarop de gecrypteerde informatie is ontsluierd. Indien de raadsman de rechtbank weet te overtuigen van mogelijke onzorgvuldigheden in het voortraject (gerede twijfel) kan de rechtbank een contra-expertise gelasten. Het O.M. dient vervolgens duidelijk te maken op welke wijze en via welke (beschreven) procedures decryptie heeft plaatsgevonden. Het proces van decryptie (gebruikte software, procedures, uitgevoerde handelingen) dient derhalve op voorhand (schriftelijk) te worden vastgelegd zodat dit bij een contra-expertise herhaald kan worden. Het lijkt mogelijk om ten aanzien van de problematiek van de contra-expertise sluitende criteria te hanteren. Immers in de Nederlandse praktijk vinden contra-expertises op zeer beperkte schaal plaats. Indien echter om contra-expertise wordt verzocht zijn de volgende opties mogelijk:

a. De rechter staat geen contra-expertise toe.
b. De rechter staat contra-expertise toe. (Vanuit exploitatie-overwegingen bestaat geen bezwaar.)
c. De rechter zal contra-expertise gelasten. (Exploitatie-overwegingen verzetten zich hiertegen, waarna de OvJ als "dominus litus" niet-ontvankelijkheid vordert. Dit is evenwel slechts mogelijk indien de bezwaren van het O.M. voor de aanvang van een terechtzitting ter kennis van de rechter zijn gebracht).

II.4.

A. Er dienen adequate financiële voorzieningen te worden getroffen.
(Het TIVC en NBV stellen bij positieve besluitvorming voorlopig gedurende één jaar capaciteit ter beschikking teneinde, in nauwe samenwerking met het GL, met de uitvoering van de geïntegreerde operationele aanpak van start te kunnen gaan.)

B. Een ambitieniveau van 80% is een vereiste.

Toelichting:

De georganiseerde criminaliteit en de politieke aktivisten blijken in Nederland op relatief grotere schaal dan in de ons omringende landen gebruik te maken van geavanceerde versluieringstechnieken van hun geautomatiseerde bestanden. Opsporings- en veiligheidsdiensten hebben nu reeds te kampen met structurele problemen waardoor criminele en politiek-aktivistische informatiestromen op onvoldoende wijze gevolgd kunnen worden. Dit leidt tot aantasting van de rechtsorde en van de veiligheid van de Staat. Daarnaast wordt ook in militaire en diplomatieke kringen steeds intensiever gebruik gemaakt van de mogelijkheden tot versluiering van gegevens. Hoewel bij TIVC, GL, BVD en NBV voldoende deskundigheid aanwezig is beschikken deze organisaties, voor de aanpak van de operationele cryptoproblematiek, over onvoldoende capaciteit. Bovendien zijn de instellingen qua organisatie niet ingericht voor de gezamenlijke aanpak van operationele problemen. Aanbevolen wordt bij TIVC, GL, BVD en NBV additionele capaciteit in mensen en middelen te creëren gericht op een geïntegreerde aanpak en waar nodig organisatorische aanpassingen aan te brengen.
Zoals reeds eerder gememoreerd, is vastgesteld dat de achterstand van de overheid groeiend is en snel zou moeten worden ingelopen, wil er uiteindelijk niet een onoverbrugbare achterstand ontstaan. De Nederlandse overheid moet in staat blijven om zelfstandig het grootste deel van de versluierde berichtgeving te ontcijferen.

Het standpunt van het ministerie van Defensie in aanmerking nemend is de Werkgroep van mening dat, gelet op de huidige verdeling van de offensieve cryptocapaciteit bij de diverse ministeries en diensten, een herschikking en herbezetting van de capaciteit niet tot oplossingen leidt. Een oplossing kan slechts gevonden worden in een verhoging van de totale capaciteit en een gestructureerde samenwerking op dit vlak tussen de betrokken ministeries en diensten. De uitbreiding van de capaciteit betreft zowel TIVC, NBV, BVD als GL waarbij structurele samenwerking tussen de diensten gestalte dient te krijgen op basis van een convenant waarin o.a. rekening wordt gehouden met de eigen taken en verantwoordelijkheden van de betrokken diensten.

Ten aanzien van het ambitieniveau gelden de volgende drie uitgangspunten:

1) het is niet realistisch om te verwachten dat 100% van de cryptoproblemen opgelost kan worden; 90% geldt als maximaal haalbaar;
2) voor een succesvolle offensieve aanpak van encryptie is een bepaalde minimale drempel (60%) in het ambitieniveau nodig;
3) een hoog ambitieniveau (80%) is een voorwaarde voor goede resultaten en vruchtbare internationale samenwerking (gebaseerd op ervaringen van het TIVC), waardoor internationale trends en technologische ontwikkelingen beter gevolgd kunnen worden.

Voor het bereiken van het vereiste ambitieniveau dient een groeipad te worden gehanteerd.
Voor het compenseren van de achterstand dient, om de startcapaciteit op een minimaal vereist peil te brengen, het ambitieniveau op tenminste 60% te worden gesteld (dit impliceert dat dan circa 60% van de ontvangen versluierde berichten ontcijferd moet kunnen worden).
Teneinde vervolgens adequaat in te kunnen spelen op de praktische operationele eisen (het onder tijdsdruk ontcijferen van versluierde berichten) en het kunnen bijhouden van de technische ontwikkelingen dient t.a.v. de capaciteit echter een "kritische massa" van 80% te worden gerealiseerd, die het noodzakelijk maakt het ambitieniveau en de daartoe noodzakelijke investeringen, geleidelijk op te voeren.
Als maximaal haalbaar geldt het niveau waarbij ca. 90% van de onder I.2.b) genoemde cryptoproblemen kan worden opgelost.
Het bijbehorende investeringsniveau beweegt zich tussen fl. 10,5 mln. (60% ontcijfering) en fl. 17 mln. (90% ontcijfering) per jaar.

Voor wat betreft de graadmeter voor de afweging tussen inspanning en resultaat kan periodiek een goede evaluatie plaatsvinden van de aangeleverde hoeveelheid versluierde berichten, het percentage ontcijferde berichten en het justitiële, beleidsmatige of preventieve resultaat van de ontcijfering. Op deze wijze kan naar behoren worden nagegaan of de verrichte organisatorische en financiële inspanningen in redelijke verhouding staan tot het verkregen resultaat, zulks gerelateerd aan het nationale belang.

In de bijlage wordt een nadere uitwerking gegeven van de consequenties van het ambitieniveau van respectievelijk 90%, 80% en 60%. Financiële, personele en materiële gevolgen zijn separaat, per organisatie weergegeven, evenals een mogelijke organisatiestructuur die hieraan gekoppeld kan worden.

II.5.

HMID, HBVD en DGPC informeren elkaar over voorgenomen en bestaande samenwerking van hun diensten met bevriende buitenlandse diensten.

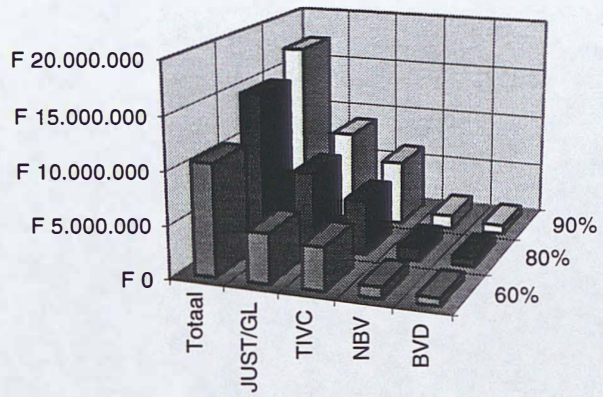
Toelichting:

Het is zeer wel mogelijk en wenselijk om nieuwe technieken te ontwikkelen in nauwe samenwerking met bevriende staten. Dat samenwerking mogelijk is wordt reeds bewezen door enige diensten ressorterend onder het ministerie van Justitie (zoals Gerechtelijk Laboratorium en KLPD) die kennis en ervaring met diensten van andere landen uitwisselen. Ook het TIVC heeft in het kader van zijn huidige taak zeer goede ervaringen op dit gebied. Voordelen van dergelijke samenwerkingsverbanden zijn (1) het beschikbaar komen van meer capaciteit voor het onderzoek naar nieuwe problemen en (2) het eerder zichtbaar worden van trends waardoor beter en sneller geanticipeerd kan worden op nieuwe ontwikkelingen. Gebleken is dat samenwerking betere resultaten afwerpt indien de nationale inbreng van kennis en kunde van een dusdanig hoog niveau is dat bevriende staten hierin geïnteresseerd zijn en blijven. De reeds bestaande internationale samenwerking dient derhalve geïntensiveerd te worden.

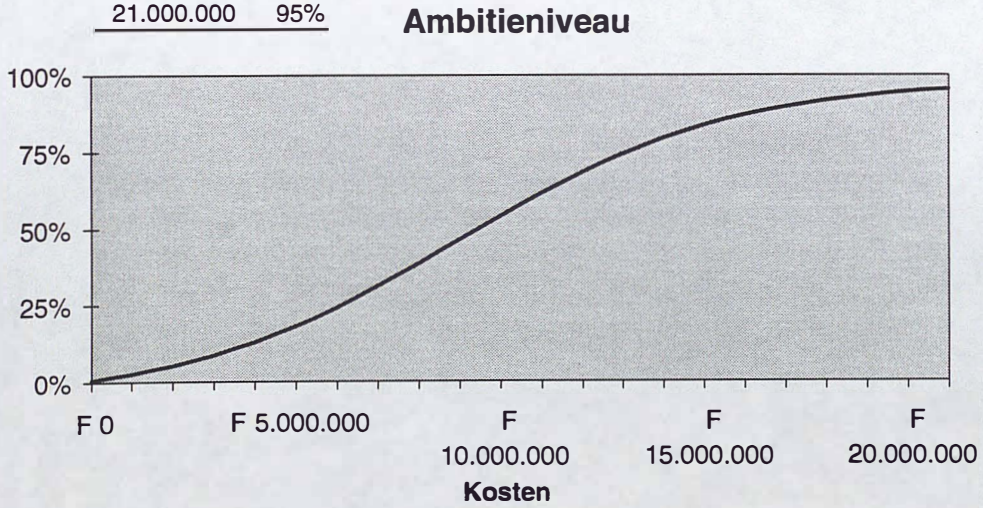
Bijlage: Onderbouwing kosten ambitieniveau 90%, 80% en 60%

Overzicht

Ambitie	TIVC	NBV	JUST/GL	BVD	Totaal
60%	4.085.000	1.072.500	4.732.500	737.500	10.627.500
80%	5.210.000	1.202.500	7.445.000	825.000	14.682.500
90%	6.265.000	1.302.500	8.810.000	850.000	17.227.500



Kosten	Ambitie
0	0%
1.000.000	3%
2.000.000	5%
3.000.000	9%
4.000.000	13%
5.000.000	18%
6.000.000	24%
7.000.000	31%
8.000.000	38%
9.000.000	46%
10.000.000	54%
11.000.000	61%
12.000.000	68%
13.000.000	74%
14.000.000	79%
15.000.000	84%
16.000.000	87%
17.000.000	90%
18.000.000	92%
19.000.000	93%
20.000.000	94%
21.000.000	95%



Ambitieniveau op 90%

Personeel	TIVC	NBV	GL/JUST	BVD	Totaal
Analyse					
Signaal	8		7		15
Crypto	7		3		10
Hardware			4		4
Software			4		4
Facilitair					
Systeembeheer	2		1		3
Administratief	1		1		2
Technisch			6		6
Planning en control					
Accountmanager	1	1	1	1	4
Operationeel			4	2	6
Offensief/defensief		3,5			3,5
Totaal fte's	19	4,5	31	3	57,5
Totaal kosten	3.515.000	832.500	5.735.000	555.000	10.637.500
Kosten manjaar	185.000				

Materiaal					
Meetapparatuur	1.000.000		1.200.000		2.200.000
Computer (15.000 MIPS)	1.500.000				1.500.000
Verbruiksgoederen	50.000		500.000	50.000	600.000
Produktie-apparatuur			1.000.000		1.000.000
Werkstations	100.000	20.000	100.000	100.000	320.000
Software	50.000	100.000	100.000	20.000	270.000
Totaal kosten	2.700.000	120.000	2.900.000	170.000	5.890.000
Projectfinanciering		300.000	125.000	75.000	500.000
Veilige Verbindingen	50.000	50.000	50.000	50.000	200.000

Overzicht 90%	TIVC	NBV	JUST/GL	BVD	Totaal
Personeel	3.515.000	832.500	5.735.000	555.000	10.637.500
Materiaal	2.700.000	120.000	2.900.000	170.000	5.890.000
Projectfinanciering	0	300.000	125.000	75.000	500.000
Veilige verbindingen	50.000	50.000	50.000	50.000	200.000
Totaal kosten	6.265.000	1.302.500	8.810.000	850.000	17.227.500

Ambitieniveau op 80%

Personeel	TIVC	NBV	GL/JUST	BVD	Totaal
Analyse					
Signaal	6		4		10
Crypto	6		3		9
Hardware			4		4
Software			4		4
Facilitair					
Systeembeheer	2		1		3
Administratief	1		1		2
Technisch			5		5
Operationeel					
Accountmanager	1	1	1	1	4
Operationeel			4	2	6
Offensief/defensief		3,5			3,5
Totaal fte's	16	4,5	27	3	50,5
Totaal kosten	2.960.000	832.500	4.995.000	555.000	9.342.500
Kosten manjaar	185000				

Materiaal	TIVC	NBV	GL/JUST	BVD	Totaal
Meetapparatuur	700.000		900.000		1.600.000
Computer (13.000 MIPS)	1.300.000				1.300.000
Verbruiksgoederen	50.000		400.000	50.000	500.000
Produktie-apparatuur			800.000		800.000
Werkstations	100.000	20.000	100.000	100.000	320.000
Software	50.000	100.000	100.000	20.000	270.000
Totaal kosten	2.200.000	120.000	2.300.000	170.000	4.790.000
Projectfinanciering		200.000	100.000	50.000	350.000
Veilige Verbindingen	50.000	50.000	50.000	50.000	200.000

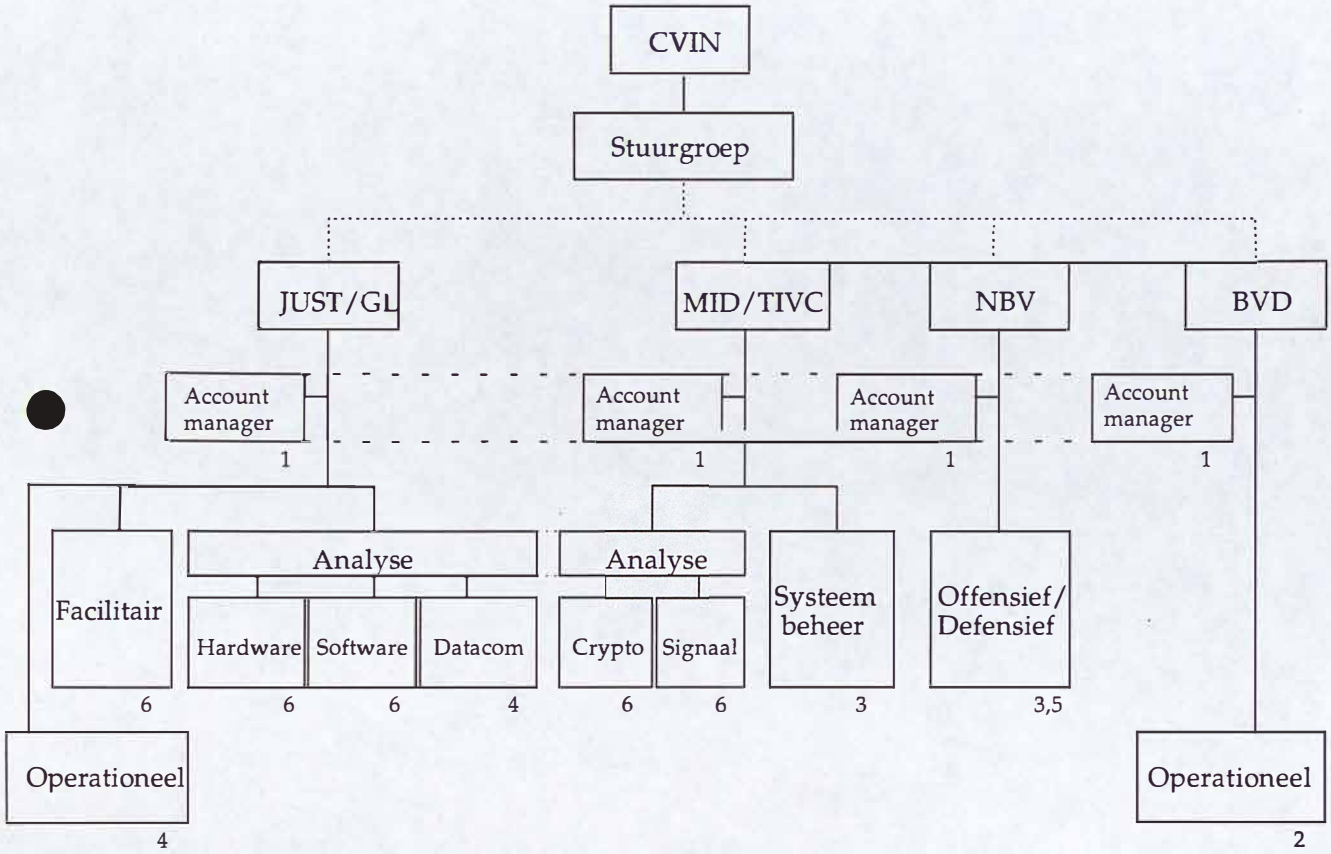
Overzicht 80%	TIVC	NBV	JUST/GL	BVD	Totaal
Personeel	2.960.000	832.500	4.995.000	555.000	9.342.500
Materiaal	2.200.000	120.000	2.300.000	170.000	4.790.000
Projectfinanciering	0	200.000	100.000	50.000	350.000
Veilige verbindingen	50.000	50.000	50.000	50.000	200.000
Totaal kosten	5.210.000	1.202.500	7.445.000	825.000	14.682.500

Ambitieniveau op 60%

Personeel	TIVC	NBV	GL/JUST	BVD	Totaal
Analyse					
Signaal	4		2		6
Crypto	5		2		7
Hardware			3		3
Software			3		3
Facilitair					
Systeembeheer	2		1		3
Administratief	1		1		2
Technisch			2		2
Operationeel					
Accountmanager	1	1	1	1	4
Operationeel			2	2	4
Offensief/defensief		3,5			3,5
Totaal fte's	13	4,5	17	3	37,5
Totaal kosten	2.405.000	832.500	3.145.000	555.000	6.937.500
Kosten manjaar	185.000				
Materiaal					
Meetapparatuur	500.000		600.000		1.100.000
Computer (10.000 MIPS)	1.000.000				1.000.000
Verbruiksgoederen	20.000		250.000	20.000	290.000
Produktie-apparatuur			500.000		500.000
Werkstations	80.000	20.000	80.000	80.000	260.000
Software	30.000	70.000	70.000	20.000	190.000
Totaal kosten	1.630.000	90.000	1.500.000	120.000	3.340.000
Projectfinanciering		100.000	37.500	12.500	150.000
Veilige Verbindingen	50.000	50.000	50.000	50.000	200.000

Overzicht 60%	TIVC	NBV	JUST/GL	BVD	Totaal
Personeel	2.405.000	832.500	3.145.000	555.000	6.937.500
Materiaal	1.630.000	90.000	1.500.000	120.000	3.340.000
Projectfinanciering	0	100.000	37.500	12.500	150.000
Veilige verbindingen	50.000	50.000	50.000	50.000	200.000
Totaal kosten	4.085.000	1.072.500	4.732.500	737.500	10.627.500

Organogram behorende bij het ambitieniveau van 80%



rd. punt 2

MINISTERIE VAN ALGEMENE ZAKEN

Kabinet van de Minister-President

Stg. CONFIDENTIEEL
Datum: 3 juli 1995
Kenmerk: 95G000074
Rubr. ambt.: Me
Einddatum rubr.: aanw. 18

Aan de leden van de MICIV

Bijgaand zend ik u de besluitenlijst van de vergadering van het CVIN-plus d.d. 3 juli 1995 t.b.v. de vergadering van de MICIV van 4 juli 1995. .

1. Cryptografie

(Bespreking covernota Coördinator en verslag Werkgroep Cryptografie)

a. Covernota

Blz 2, regel 8/9: in plaats van "jaarlijkse investering" dient gelezen te worden:"jaarlijkse inspanning".

b. Verslag Werkgroep Cryptografie (Beslispuntennota)
-Beslispunt II.1:

Bij de evaluatie van de overeenkomst tussen de Staat en Philips Crypto dient het CVIN betrokken te worden ten aanzien van de relatie tot de operationele aanpak van de cryptoproblematiek. De evaluatie dient eind 1995 aan te vangen en moet medio 1996 worden afgerond.

-Beslispunt II.4:

1e. Het CVIN-plus stelt voor met ingang van 1 januari 1996 te starten met het voorgestelde samenwerkingsverband tussen de betrokken diensten voor een proefperiode van een jaar. In het midden van deze proefperiode zal de samenwerking nader worden geëvalueerd opdat de MICIV medio 1996 een besluit over de voortzetting van het samenwerkingsverband kan nemen.

2e. De financiering van het samenwerkingsverband zal voorshands exogeen moeten geschieden tenzij hiervoor ruimte kan worden gevonden in het actieprogramma Electronische Snelweg danwel onder het ICES-programma.

Postbus 20001 - 2500 EA 's-Gravenhage - Kantooradres: Binnenhof 20 - Tel. 070-3564100 - Fax 070-3564683

In het proefjaar kan worden volstaan met een bedrag dat overeenkomt met een ambitieniveau van 60% (ca. 9,5 mln.). Bij positieve besluitvorming over voortzetting van de samenwerking zal de jaarlijkse inspanning moeten doorgroeien naar een ambitieniveau van 80% (ca 13 mln.).

3e. De aansturing en de organisatiestructuur van het samenwerkingsverband zal nader worden uitgewerkt door het CVIN.

2. Non-proliferatie
(Oprichting interdepartementale werkgroep)

BZ en BVD zullen onderling overleggen over het voorzitterschap van deze werkgroep.

De coördinator van de
inlichtingen- en
veiligheidsdiensten,

mr. J.P.M.H. Merckelbach