Minister EZ

Nota

Ministerie van Economische Zaken

Auteur
drs J.A.M. Obdeyn

Datum
3 juli 1995

Aan
de Minister

Toestelnummer
6263

Uiterlijk bij geadresseerde

Notanummer
BEb/DHZ/SGS
95046537

Informatiekopie aan
Archief

Bijlage(n)

Medeparaaf en datum

Onderwerp
Beslispuntennota m.b.t. operationele cryptoproblematiek (MICIV 769-95)

Samenvatting en conclusies

1. Probleemstelling

Tot voor enige jaren behoorde het ver- en ontsluieren van informatie tot het primaat van de inlichtingendiensten. De snelle ontwikkelingen op het gebied van de telecommunicatie en de computertechnologie hebben echter geleid tot een toenemend gebruik van cryptografie op de zakelijke en consumentenmarkt. Het economisch-maatschappelijk belang van cryptografie is steeds zwaarwegender geworden t.o.v. het staatsveiligheidsbelang.

Vanuit de instanties verantwoordelijk voor het staatsveiligheidsbelang zijn, globaal gesproken, drie reacties waar te nemen:

- inspanningen tot het opleggen van beperkingen op de toepassing en de export van cryptografie in de commerciële sector;
- instandhouden van een nationale crypto-industrie en het ontwikkelen van "overheidsvriendelijke" crypto;
- verschaffen van de middelen aan de inlichtingendiensten en de opsporingsinstanties om versluierde informatie toegankelijk te maken.

Deze laatste reactie is, met als onderwerp "operationele aanpak", nu aan de orde in de CVIN-plus en de MICIV.

2. Uitgangspunt en conclusies

De MICIV heeft op 24 jan. 1995 aan de CVIN opdracht gegeven oplossingen te zoeken waarbij een gezamenlijke aanpak op operationeel-technisch terrein en een optimale benutting van de bij de inlichtingen- en opsporingsdiensten aanwezige capaciteit als uitgangspunt geldt. De CVIN heeft een "Werkgroep Cryptografie" opdracht gegeven een beslispuntennota op te stellen.

Ontvangen *Verzonden* *Terugontvangen* Paraaf en datum

In te vullen door Secretariaat Generaal

04.00.ALG.

De opgestelde beslispuntennota kent echter twee belangrijke beperkingen:

- Geconstateerd wordt dat de sterke groei en complexiteit van de cryptoproblemen een nationale geïntegreerde aanpak vereist, bestaande uit een nauwe samenwerking tussen BVD (BiZa), TIVC (Def), Gerechtelijk Laboratorium (Just) en NBV (Def en BZ). De verschillende belangen van de bij de cryptoproblematiek betrokken overheidsdiensten blijken echter groot te zijn. Zo is herverdeling en herbezetting van capaciteit voor het ministerie van Defensie niet bespreekbaar;
- Geconstateerd wordt dat het opsporings- en veiligheidsbelang vereisen dat circa 80% van de aangeboden versluierde berichten d.m.v. ontcijfering tijdig leesbaar moet worden gemaakt. Dit ambitieniveau van 80% lijkt onvoldoende aannemelijk te worden gemaakt.

De conclusie in de nota dat een extra budget van circa fl. 14,5 miljoen per jaar noodzakelijk is om de verschillende diensten van extra middelen en mankracht te voorzien, is daardoor niet goed onderbouwd. Verder wordt niet aangegeven hoe dit bedrag budgetair geregeld dient te worden.

3. Beslispunten

Beslispunt II.1: EZ van mening dat een nationale zelfscheppende crypto-industrie levensvatbaar moet zijn.

Beslispunt II.2: EZ van mening dat wettelijke maatregelen de commerciële ontwikkelingen niet onnodig dienen te beperken.

Beslispunt II.3: EZ van mening dat de beslissingsbevoegdheid van de CVIN op het terrein van de cryptoproblematiek nader moet worden omschreven en er geen overlapping zou moeten optreden met bijv. de Interdepartementaal Overleg Vergunningen en Controlebeleid (IOVC, vz. EZ).

Beslispunt II.4: EZ van mening de relatie *nationale samenwerking-ambitieniveau-adequate financiele voorzieningen* niet voldoende is toegelicht.

Beslispunt II.5: Geen commentaar.

Voorafgaande de MICIV zal ik u mondeling op de hoogte brengen van het verloop van het hedenmiddag plaatsvindende voorbereidend overleg in de CVIN-plus.

drs F.A. Engering
directeur-generaal van de
Buitenlandse Economische Betrekkingen

21

MINISTERIE VAN FINANCIEN. CONFIDENTIEEL
Memo d.d. 6 juli 1995

In de MICIV-vergadering van 4 juli jl. is mij gevraagd een voorstel aan de Raad te doen voor de financiele dekking van de noodzakelijk geachte oplossing van de zgn. cryptoproblematiek.
Bij onderstaand voorstel heb ik de volgende uitgangspunten gehanteerd:

- in het proefjaar 1996 kan worden volstaan met een begrag dat overeenkomt met een ambitieniveau van 60 % (9,3 mln.[1]).
- bij positieve besluitvorming over de voortzetting van de samenwerking (medio 1996 te beslissen) zal de jaarlijkse inspanning kunnen doorgroeien naar een ambitieniveau van 80 % in 1997 (13,0 mln.[1]) en 90 % in 1998 (15,2 mln[1])
- de betrokken departementen Justitie, Defensie en BiZa dragen naar rato bij in de te maken investerings- en exploitatiekosten nadat deze eerst zijn verlaagd met een bijdrage van EZ uit de clusterIII-gelden (electronic highway-) en van Financien (25 % van het dan resterende bedrag).

De bovenstaande uitgangspunten leiden tot het volgende voorstel ten aanzien van de kostenverdeling:

	1996 (60%)	1997 (80%)	1998 e.v. (90%)
Totale kosten	9,3	13,0	15,2
waarvan:			
EZ	1,0	3,0	3,0
resteert	8,3	10,0	12,2
Financiën 25%	2,1	2,5	3,1
resteert	6,2	7,5	9,1
naar rato:			
Justitie	3,1	4,1	5,1
Biza	0,5	0,5	0,5
Defensie	2,6	2,9	3,5
Totaal	9,3	13,0	15,2

---

[1] Dit bedrag is afgeleid van de bedragen genoemd in stuk nr. 95G000069; er heeft een kleine neerwaartse technische bijstelling plaatsgevonden.

Genoemde meerkosten voor het cryptoprogramma zullen binnen de begrotingen van de genoemde departementen moeten worden opgevangen, (specifieke compensatie), bij voorkeur binnen een personeel/materieel artikel.

Tot slot lijkt van belang dat de betrokken bewindslieden instemmen met de voorgestelde herschikkingen van de middelen en toezeggen dat ze binnen de aangegeven tijdpaden de voorgestelde activiteiten, onder de coördinerende leiding van het CVIN, zullen ontplooien.

-o-

MICIV 76g-95
4-7-95-2

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

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.

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.

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.

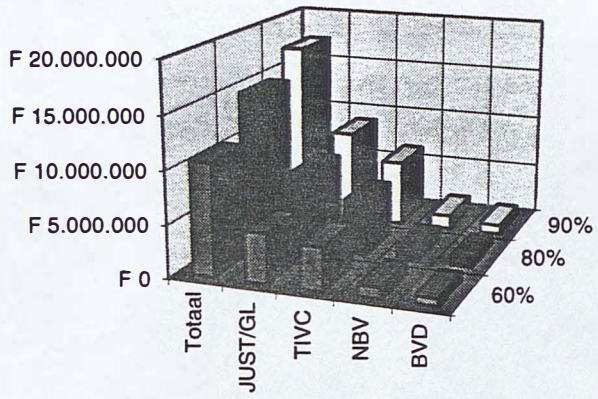
Toelichting:

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.

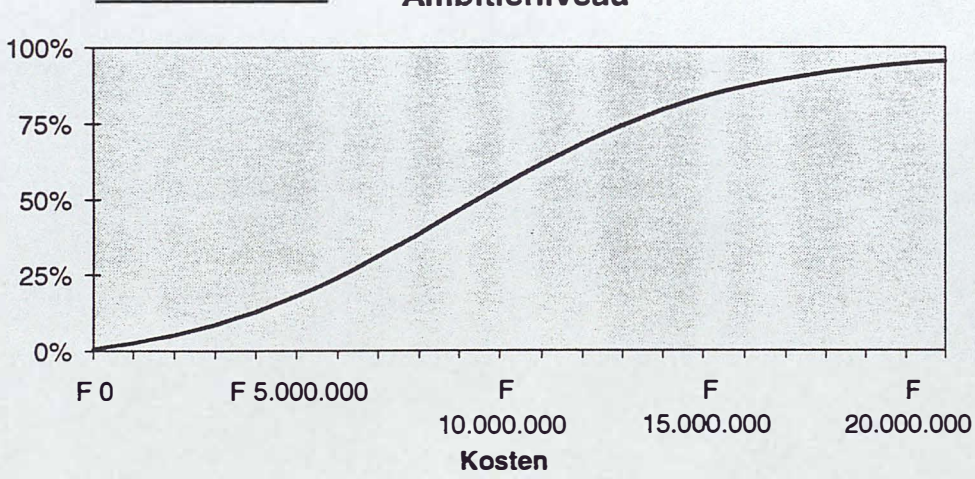
Bijlage: Onderbouwing kosten ambitieniveau 90%, 80% en 60%

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%