17

16a

MINISTERIE VAN ALGEMENE ZAKEN

Kabinet van de Minister-President

[redacted]

Nr. Alk 4663

Aan: Hoofd BVD
Hoofd IDB
Hoofd MID
CVIN.vert. BuZa
c.c.: [redacted]
H-NBV- BuZa.

Betreft: Crypto-apparatuur
Bijlage: nota

's-Gravenhage, 17 november 1988

Hierbij bied ik u in bijlage aan een aantekening van hoofd Nationaal Bureau voor Verbindingsbeveiliging (NBV) betreffende de verspreiding van crypto-apparatuur.

Zoals reeds door mij aangegeven, zal een eerste gedachtenwisseling over het onderwerp plaatsvinden in de CVIN-vergadering van 14 december a.s.

Ik stel voor het hoofd NBV bij de behandeling van het onderwerp uit te nodigen. De aanwezigheid van andere experts lijkt mij voorshands nog niet nodig.

De Coördinator voor de
Inlichtingen- en
Veiligheidsdiensten,

F.H. Alkemade, Gen.Maj. b.d.

[redacted]

Alk/Pl

Postbus 20001 – 2500 EA 's-Gravenhage – Kantooradres: Binnenhof 20 – Tel. 070-614031

Bijlage

Verspreiding Crypto-apparatuur

1. SAMENVATTING

In deze aantekening zal worden aangegeven dat er met betrekking tot de handel in crypto-apparatuur in Nederland een situatie dreigt te ontstaan die volledig verschilt van die bij de grote NAVO bondgenoten.
Deze situatie zal zeer ten nadele kunnen werken van onze verhoudingen in het telematica beveiligings- en inlichtingenveld met die bondgenoten, aangezien hun inlichtingenbelangen en ook die van ons kunnen worden geschaad.

Deze situatie ontstaat
a. doordat een aantal firma's zich nieuw met de produktie van crypto-apparatuur gaat bezighouden, gegeven het feit dat de behoefte aan die apparatuur toeneemt en de produktie door de voortschrijdende techniek eenvoudiger wordt;
b. doordat een duidelijk mandaat en de capaciteit ontbreekt om de produktie en handel door de industrie vanwege de overheid te laten begeleiden.

2. ENKELE GEGEVENHEDEN

a. De eenvoudigste, meest profijtelijke en risicoloze manier om inlichtingen te verkrijgen is via het afluisteren van verbindingen en het "breken" van de vercijfersystemen van de opponent. Deze vorm van inlichtingen verzamelen wordt op grote schaal toegepast door bijvoorbeeld de US (NSA), het UK (GCHQ), de BRD (ZfCh).

b. Er bestaan twee soorten crypto-apparatuur.

High-grade crypto-apparatuur

Dit is crypto-apparatuur waarin, naar de stand van de modernste techniek, cryptosystemen zijn ingebouwd die het onmogelijk maken dat uit de verzonden signalen nog informatie is te verkrijgen, ook niet met de meest geavanceerde en duurste analytische computersystemen. Deze apparatuur wordt gebruikt voor overheids- en/of NAVO-verbindingen.
Op de vrije markt zijn apparaten met deze systemen niet of nauwelijks te verkrijgen omdat de exportwetten van de meeste crypto-apparatuur producerende landen de uitvoer van deze apparatuur verbieden.

"Commerciële" crypto-apparatuur

Met deze term wordt crypto-apparatuur aangeduid waarvan de cryptografische sterkte kunstmatig lager wordt gehouden om export mogelijk te maken.

c. De verdeling commerciële crypto versus overheidscrypto heeft tot doel om aan terroristen, drughandelaren, buitenlandse regeringen die zulke aktiviteiten steunen en regeringen die potentieel vijanden zijn, de mogelijkheid te onthouden de verbindingen dusdanig te beveiligen dat de westerse overheden er ook met grote inspanning niet meer in zouden slagen de verbindingen mee te lezen. De commerciële apparatuur biedt aan normale gebruikers voldoende bescherming, omdat de "tegenstander" niet de vele miljoenen guldens op tafel zal leggen, en niet de kennis heeft, die nodig is om "in te breken".

d. Hoe bereikt men dat de sterkte van de cryptologics in commerciële apparatuur kunstmatig laag gehouden wordt? Voor wat betreft de verkoop binnen de landsgrenzen kan men naar de US als voorbeeld kijken. Vertegenwoordigers van NSA zijn een groot deel van hun tijd bezig om crypto-firma's duidelijk te maken dat het in het belang van de nationale veiligheid is om medewerking te verlenen. Vrij openlijk wordt duidelijk gemaakt waarom het gaat en wordt met enige nadruk de goede verstandhouding tussen de firma en de overheid ter sprake gebracht. Naar verluid zijn op deze wijze in de laatste jaren honderden firma's bezocht waarbij slechts drie firma's onwillig bleven om mee te werken. In andere landen lijkt men op dezelfde wijze tewerk te gaan. Ook in Nederland bestaan geen wettelijke middelen om verkoop in Nederland van in Nederland aangemaakte crypto aan subversieve elementen tegen te gaan. Een "overredingsbeleid" van fabrikanten schijnt het enige wapen daartegen.

e. De exportwetten.
Door het Uitvoerbesluit Strategische Goederen 1963 dat gebaseerd is op de In- en Uitvoerwet is de regering in staat de export van crypto-apparatuur te reguleren. De apparatuur valt onder artikel 1527 of artikel 11 van de bij het besluit gevoegde lijst (COCOM-lijst).
Alle westerse landen, met een enkele uitzondering, hanteren zulke lijsten die in "COCOM-verband" (NAVO-landen en Japan) op elkaar worden afgestemd.

f. De firma Philips Usfa heeft een kontrakt met de Staat (waarbij de NVBR voor de Staat optreedt), waarin de vrijheid van verkoop van crypto dusdanig aan banden wordt gelegd, dat wij er zeker van zijn dat Usfa, waar toepasselijk, slechts commerciële crypto exporteert.

3. HET PROBLEEM

a. Aan de overzichtelijke situatie dat Usfa de enige crypto-producent in Nederland was die bovendien door de Staat wordt gecontroleerd, lijkt een einde te komen doordat een aantal firma's zich aandient als producent van high-grade crypto-apparatuur:

(1) de PTT met de firma CONTEST (voorheen CWP) die een high-grade crypto in 1989 gaat uitbrengen met de naam TIRO en nog verder plannen heeft.

(2) RVO-TNO die in opdracht van de KL een high-grade crypto in een data terminal aan het ontwikkelen is.

(3) HSA die apparaten gaat verkopen waarin crypto is opgenomen.

(4) Philips International die er naar tendeert om "veiligheids"- ontwikkelingen bij MBLE in België te doen plaatsvinden.

(5) de firma Anchor Datacom die een modom met sterke crypto in NL heeft ontwikkeld en in NL gaat aanmaken en verkopen.

b. Naar nu ook blijkt is de exportwetgeving in Nederland op het gebied van crypto-apparatuur niet waterdicht.
In de considerans van het Uitvoerbesluit Strategische Goederen is slechts sprake van "het belang van de internationale rechtsorde" en niet langer zoals wel in de In- en Uitvoerwet "het belang van de inwendige en uitwendige veiligheid des lands".
Economische Zaken betwijfelt of op basis van de considerans van het Uitvoerbesluit de export van high-grade crypto-apparatuur van genoemde firma's kan worden tegengehouden.
In UK en US gaat geen crypto-exportvergunning betreffende crypto de deur uit voordat GCHQ c.q. NSA zijn handtekening heeft gezet.