Problematiek betreffende crypto-apparatuur

Algemeen

Een zeer belangrijke en tegelijk veilige manier om inlichtingen te verzamelen is het afluisteren van de (overheids)verbindingen van potentiële tegenstanders na "kraking" van toegepaste cryptosystemen.
Deze vorm van inlichtingen verzamelen wordt door vele landen toegepast, waarbij elke overheid zich ook realiseert dat de eigen verbindingen eveneens doelwit zullen zijn van afluisteractiviteiten van andere landen.

Men onderscheidt twee categorieën crypto-apparatuur:

- high-grade 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. Binnen de NAVO wordt dit soort apparatuur door overheden gebruikt voor de beveiliging van de eigen en/of NAVO-verbindingen. Op de internationale vrije markt is deze apparatuur niet te verkrijgen omdat de exportwetten van de meeste crypto-apparatuur producerende landen de uitvoer van dit soort apparatuur verbieden (COCOM).

- commerciële crypto-apparatuur, waarvan de cryptosterkte kunstmatig lager wordt gehouden dan die van high-grade apparatuur. Voor deze apparatuur geldt geen of een milder COCOM-regime en export is in het algemeen mogelijk. Deze apparatuur biedt normale gebruikers voldoende bescherming tegen bijv. concurrenten, maar ontneemt terreurorganisaties en drugssyndicaten de mogelijkheid hun verbindingen zodanig te beveiligen dat politie en/of veiligheidsdiensten niet zouden kunnen "inbreken".

Commerciële apparatuur laat zich vaak moeilijk onderscheiden van high-grade apparatuur en het vereist in ieder geval veel technische kennis om de cryptografische sterkte (het bestaan van "lekken") vast te stellen.

Een overheid kan eigenlijk alleen maar zeker zijn van de betrouwbaarheid van te gebruiken cryptosystemen indien deze in eigen land hetzij door de overheid zelf, hetzij onder strenge overheidscontrôle worden geproduceerd.

Situatie in Nederland

De beveiliging van de overheidsverbindingen in Nederland is een taak van de Nationale Verbindingsbeveiligingsraad (NVBR), ingesteld bij beschikking van de ministers van Buitenlandse Zaken en Defensie, en van het Nationaal Bureau Verbindingsbeveiliging (NBV).
De NVBR is onder meer belast met het voorbereiden van het overheidsbeleid terzake, terwijl het NBV als uitvoerend orgaan belast is met alle (technische) crypto-aangelegenheden van de gehele rijksoverheid.

Negatieve ontwikkelingen

Aan de overzichtelijke (en comfortabele) situatie dat USFA de enige high-grade cryptoproducent in Nederland is lijkt een einde te komen. Andere firma's, waaronder de PTT met de firma CONTEST, RVO/TNO, Philips/HSA en ANCHOR DATACOM, dienen zich aan als producent en naar mag worden aangenomen als exporteur van high-grade cryptosystemen.
Zoals reeds eerder opgemerkt is valt deze apparatuur onder het COCOM-regime, met andere woorden voor export zal een vergunning moeten worden aangevraagd bij het ministerie van Economische Zaken.

Zoals in andere landen het geval is en in ieder geval in de VS, UK en BRD (partners in vierlanden-overleg) zijn ook de voorzitter NVBR, het NBC en het CVIN van mening dat export van high-grade crypto ongewenst is en dat dientengevolge een exportvergunning zou moeten worden geweigerd. Deze mening is overigens nimmer in de praktijk getest, aangezien de noodzaak hiertoe niet bestond omdat het contract Staat-USFA voldoende mogelijkheden bood om ongewenste ontwikkelingen te voorkomen. Indien een dergelijk "contractsysteem" ook met de hierboven genoemde firma's wordt aangegaan kan de export van high-grade crypto op dezelfde wijze als in het geval van USFA worden voorkomen/gecontroleerd.
Indien een dergelijk contractsysteem niet mogelijk zou zijn - en dezerzijds bestaan gerede twijfels - vormt het Uitvoerbesluit Strategische Goederen de laatste mogelijkheid om export van high-grade crypto te voorkomen.

Naar nu echter blijkt is deze exportwetgeving in Nederland niet sluitend. In de considerans van genoemd besluit is namelijk slechts sprake van "het belang van de internationale rechtsorde" en niet langer zoals wel in de In- en Uitvoerwet "het belang van de volkshuishouding, van de inwendige en uitwendige veiligheid des lands en van de internationale rechtsorde".
Economische Zaken betwijfelt of op basis van de huidige considerans van het Uitvoerbesluit de export van high-grade crypto-apparatuur kan worden tegengehouden. Daarbij komt dat formeel uitsluitend de minister van Economische Zaken bevoegd is uitvoervergunningen te verlenen c.q. te weigeren, waarbij slechts in bepaalde gevallen het advies van de minister van Buitenlandse Zaken wordt ingewonnen. De minister van Defensie wordt in het geheel niet geraadpleegd, terwijl in praktisch alle gevallen crypto een militaire toepassing heeft c.q. kan hebben. Evenmin zijn de NVBR, het NBV en de inlichtingen- en veiligheidsdiensten bij de procedure betrokken.

- Opgemerkt wordt -

Opgemerkt wordt dat de VS, UK en BRD op het gebied van de verbindingsinlichtingen zeer veel geïnvesteerd hebben in personeel en materieel. Indien door een niet sluitende exportwetgeving in Nederland high-grade cryptosystemen op de internationale markt zouden komen waardoor deze investeringen zouden worden gefrustreerd, laten de gevolgen voor het vierlanden-overleg zich gemakkelijk raden: op het gebied van verbindingsinlichtingen/veiligheid zal Nederland als "onbetrouwbaar" worden aangemerkt met mogelijke nadelige gevolgen op andere gebieden van (inlichtingen)samenwerking.

Aanbevelingen

De belangrijkste voorwaarde voor het vinden van een oplossing voor de geschetste problematiek is erkenning door betrokken ministers (MICIV) dat beheersing van de proliferatie van high-grade cryptosystemen een nationaal belang is. Dit belang - het zij nogmaals vermeld - betreft de taakuitvoering door de inlichtingen- en veiligheids-diensten en de relaties met NAVO-bondgenoten.

Uitgaande van deze erkenning komt het CVIN tot de volgende aanbevelingen:

- als algemene en bindende regel geldt dat de export van high-grade crypto in principe verboden is. Slechts in zeer bepaalde gevallen (zie bijlage) wordt vergunning verleend.

- Onder handhaving van de autonome bevoegdheid van de minister van Economische Zaken betreffende het verlenen c.q. weigeren van exportvergunningen en onder handhaving van de in bepaalde gevallen noodzakelijke raadpleging van Buitenlandse Zaken (DAV), wordt voor wat betreft de export van crypto-apparatuur in alle gevallen ook de minister van Defensie bij de advisering betrokken, gezien het feit dat crypto-apparatuur in nagenoeg alle gevallen ook "militair" kan worden gebruikt.

- Het advies ten behoeve van de minister van Defensie wordt opgesteld door H-MID in nauwe samenwerking met het NBV dat belast wordt met het technisch onderzoek van voor export aangeboden apparatuur. Hiertoe zal de organisatie van het NBV moeten worden versterkt.

- het onderzoek door het NBV kan uitwijzen:

  - de exportaanvraag betreft high-grade crypto. In dat geval gelden de regels als vermeld in bijlage.

  - de exportaanvraag betreft commerciële crypto, echter wel vallend binnen de beschrijving van crypto zoals opgenomen in de bijlage bij het Uitvoerbesluit Strategische Goederen en dus een COCOM-artikel.

- In dat geval -

In dat geval wordt het Defensie-advies in de besluitvorming van Economische Zaken betrokken, echter de minister van Economische Zaken beslist.

- de export-aanvraag betreft commerciële crypto, echter niet vallend binnen de beschrijving als in voorgaand punt bedoeld, derhalve geen COCOM-artikel en dus geen vergunning nodig.

- In geval de MICIV deze aanbevelingen overneemt, het CVIN belasten met de verdere uitwerking van procedures/voorstellen waartoe vertegenwoordigers van Economische Zaken en van het NBV bij het overleg terzake zullen worden uitgenodigd.

19 april 1989
Alk