DE KWALITEIT VAN DE INFORMATIEVOORZIENING.

"De juiste informatie op de juiste tijd en op de juiste plaats".

Door: Ing. B.J. van Maaren en Lkol M.C. van Riemsdijk MBT
Directie Informatievoorziening en Organisatie
van de Centrale Organisatie Ministerie van Defensie.

VOORWOORD

In deze bijdrage wordt ingegaan op het (centrale) beleid ten aanzien van de informatievoorziening (IV) van het ministerie van defensie, het management hiervan met het zgn. programmamanagement en de plaats van de informatiebeveiliging in dit beleid. Bovendien wordt ingegaan op een aantal projecten voor informatiebeveiliging die door de Directie Materieel KL in opdracht van de Beveiligingsautoriteit zijn begeleid in samenwerking met alle defensieonderdelen en enkele ministeries: de V-kaart en gerelateerde projecten, het zogenaamde TIBI-concept voor pc-beveiliging, netwerkbeveiliging en cryptosleutelmanagement.
Twee jaar geleden is in Intercom (juni 1999) reeds een artikel gepubliceerd waarin de samenhang van de TIBI-producten werd beschreven. Het Parlement is op 17 oktober 2001 door de Staatssecretaris is geïnformeerd over de stopzetting van de ontwikkeling van deze producten.
Als alternatief voor het TIBI programma is, op voorstel van de Beveiligingsautoriteit, door het Politiek Beraad o.l.v. de Minister in augustus 2000 een meer geleidelijk programma vastgesteld. Dit programma maakt deel uit van het in september 2000 vastgestelde programmamanagement voor de defensiebrede informatievoorziening waarover hieronder meer . Vervolgens wordt het informatiebeveiligingsbeleid aangehaald waar informatiebeveiliging als randvoorwaarde (en dus ook als kwaliteitsfactor) bij de informatievoorziening onlosmakelijk hoort. Als laatste worden de “lessons learned” uit het project V-kaart weergegeven.

KWALITEIT VAN DE INFORMATIEVOORZIENING

Wat is kwaliteit van de informatievoorziening (IV)? In de eerste plaats houdt dit in dat het proces van de commandovoering en de bedrijfsvoering altijd kan beschikken over de gevraagde informatie (doeltreffendheid). Bovendien moet deze informatie op de juiste tijd (dus niet te vroeg of te laat) en op de juiste plaats (uitsluitend bij de geadresseerden en niet bij degene die er geen recht op heeft) beschikbaar zijn. Dit betekent dus dat informatie aan zekere betrouwbaarheidseisen moet voldoen wil het geschikt zijn voor het bedoelde proces. De betrouwbaarheid wordt uitgedrukt in een mate van exclusiviteit (confidentiality), volledigheid (integrity) en beschikbaarheid (availability). Daarmee ontstijgt beveiliging de vaak gebruikte misvatting dat beveiliging synoniem zou zijn met “goed opbergen”. Ook de factor beschikbaarheid is zeer van belang voor de kwaliteit van de informatievoorziening!
Kortom: de juiste informatie op de juiste tijd op de juiste plaats is een zaak van de informatiebeveiliging en geeft kwaliteit aan de informatievoorziening.

HET PROGRAMMAMANAGEMENT VAN DE INFORMATIEVOORZIENING

Het sturingsconcept van Defensie, “centrale regie en decentrale uitvoering” moet ertoe bijdragen dat de organisatie - ondanks de verscheidenheid van de samenstellende delen - een eenheid vormt die doelmatig en doeltreffend functioneert en daarover op controleerbare wijze verantwoording aflegt. Het veranderingsproces vergt op veel fronten bijsturing, aanpassing en aanvullende initiatieven, zowel bij mensen als in de werkomgeving. Technologische hulpmiddelen zijn hierbij van groot belang. Informatie- en communicatietechnologie (ICT) is onmisbaar voor de informatievoorziening (IV) in elke moderne organisatie, Defensie niet uitgezonderd. Dankzij moderne ICT kan informatie snel op veel plaatsen beschikbaar zijn. Hierdoor worden niet alleen de besturingsmogelijkheden versterkt, maar kan ook de interne communicatie relatief eenvoudig worden verbeterd.
Door de stormachtige ontwikkelingen in de ICT kunnen echter ook ongewenste effecten optreden, zoals de fragmentatie van de middelen waardoor juist de doorzichtigheid wordt belemmerd. In de komende jaren is daarom standaardisatie de norm en zal het beleid voor de informatievoorziening centraal door het kerndepartement worden vastgesteld.

> *”als ik me realiseerde hoe defensiesystemen in elkaar steken en bedacht dat op talloze plaatsen iets chipachtigs zit, dat van alles werkt met computers, met nullen en enen, dan verrraste me dat aantal niet. Het heeft er ook mee te maken dat defensie de problematiek uiterst grondig aanpakt. In de Kamer heb ik gezegd dat zelfs flipperkasten in soldatenkantines zijn geïnventariseerd.”*
>
> *Staatssecretaris Van Hoof (Computable)*

Bovenstaande tekst is een citaat uit het beleidsplan voor de informatievoorziening van defensie: het IV-beleidsplan. Dit beleidsplan is in mei van dit jaar door de Minister vastgesteld en behandelt de centrale beleidsontwikkeling, planning en control van de IV. De IV voor defensie, dus de IV ten dienste van de bedrijfsvoering maar ook voor de commandovoering, wordt samengevat in een aantal doelstellingen, de te realiseren activiteiten om de doelstellingen te bereiken en de beschikbare middelen hiervoor (de te reserveren budgetten). Een en ander geschiedt in overeenstemming met de rijksbrede policy “Van Beleidsbegroting tot Beleidsverantwoording (VBTB)”. VBTB is bedoeld om beslissingen te kunnen toetsen aan het beleid en verantwoording te kunnen afleggen aan het Parlement. Dat betekent dat aan de uitvoering van beleid vragen zijn gekoppeld: wat willen we bereiken (doelstelling), wat zullen we daar voor doen (activiteiten) en wat hebben we daar voor over (middelen)? Militair gezien lijkt dit voor de hand te liggen (zie het ons bekende Operationeel Besluitvormingsproces(OBP)), de politiek was echter nog niet zover! Nu is de begroting van defensie voor het eerst geschreven in deze lijn, waardoor parlementaire controle door het meten van de realisatie (de effectiviteit) van de doelstellingen mogelijk is.
Op deze manier is dus het IV-beleidsplan conform VBTB opgesteld, voor de eerste keer in het eerste kwartaal van dit jaar. In

mei van dit jaar is dit beleidsplan in het Politiek Beraad behandeld en goedgekeurd door de Minister. Als volgende stap is dit beleid vertaald naar doelstellingen voor de komende 5 jaar en vervolgens vertaald naar activiteiten voor het jaar 2002. Deze activiteiten zijn door middel van het zgn. IV-uitvoeringsplan verbonden aan de begroting voor komend jaar. Gedurende het jaar 2002 zal de uitvoering van dit plan worden gevolgd en waar nodig worden bijgesteld

De basis van het programmamanagement wordt gevormd door gemeenschappelijke (defensiebrede) en gezamenlijke (joint) ontwikkelingen die zoveel als mogelijk en nodig zijn gestoeld op bestaande producten van de plank, zoals commercial, governmental of military off the shelf (COTS, GOTS, MOTS). Om op beheerste wijze invulling te kunnen geven aan behoeftestellingen op informatievoorzieninggebied is de complexe materie verdeeld in overzichtelijke programma's met projecten of activiteiten die een zekere onderlinge relatie hebben. Deze programma's zijn complementair en omvatten samen het gehele IV-spectrum dat voor Defensie van belang is. De uitvoering van de projecten en activiteiten berust op een zo generiek mogelijke opzet: in beginsel wordt per functionele informatiebehoefte slechts één applicatie of systeem actief. Vanzelfsprekend kan niet alles tegelijkertijd worden aanbesteed of uitgevoerd. Dit zou financieel onhaalbaar zijn en fysiek onuitvoerbaar. Voorts moeten sommige activiteiten aan andere vooraf gaan. Projecten zullen dan ook in een zekere volgorde worden uitgevoerd. Dit vereist een meerjarig plan met een strakke (centrale) regie en voldoende terugkoppeling tijdens de uitvoering om tijdig te kunnen beoordelen of bijsturing nodig is. Dit is in het IV-beleidsplan vastgelegd. De IV-beleidsontwikkeling, planning en begroting, opdrachtgeving voor realisatie, en de IV-Control is neergelegd bij de Directie Informatievoorziening en Organisatie (DIO) van het kerndepartement. Deze directie is op 13 september 2001 formeel opgericht en is voortgekomen uit elementen van de Directie Economie & Financiën (DGEF) en de afdeling CIS van de Defensiestaf plus een vijftal nieuwe functies.Het doel van het IV-beleidsplan is:

- het definiëren van de programma's;
- het stellen van doelen per programma;
- het beschrijven van de samenhang (architectuur) tussen deze programma's;
- het beschrijven van een uitvoeringsstrategie;
- het definiëren van bevoegdheden en verantwoordelijkheden;
- het vaststellen van een kader om initiatieven en behoeftestellingen te kunnen toetsen.

Alle IV-ontwikkelingen zijn gebaseerd op een gezamenlijke architectuur die, met het Project Herinrichting Informatievoorziening Defensie PHIDEF, in 1998 is ontwikkeld: de Defensie Informatie Architectuur DIA. In 1999 zijn daaruit tien elkaar aanvullende IV-programma's ontwikkeld voor het totale IV-veld. Deze tien programma's en enkele daarbinnen te vatten projecten zijn:

- ICT-Infrastructuur (NAFIN, LAN2000);
- Operationele IV (TITAAN, MilSatCom);
- Documentaire IV (X-Post);
- Standaard IV (ERP);
- Personele IV (HRM, P&O2000+);
- Materieellogistieke IV (CVBKL, BBS);
- Financiële IV (GVKKA, Finad2000);
- Medische & Arbo IV (GDBK, GIFKOM)
- IV voor Opleidingen;
- Informatiebeveiliging (2 Mb Vcf, VIR)

Om het beleid dat uitgangspunt is voor de informatievoorziening deels functioneel is, is per programma een zgn. Beleidsverantwoordelijke aangesteld die verantwoordelijk is voor dit functionele beleid maar ook voor het IV-beleid binnen die functie.

Deze Beleidsverantwoordelijken zijn: CDS (operationeel), DGEF (financieel), DGP (personeel), DGM (matlog) en de Beveiligingsautoriteit; bovendien is de DGEF Beleidsverantwoordelijke voor de Standaard IV en voor de samenhang tussen de programma's of wel de architectuur. De DGEF vervult dan ook de rol van I-manager van het ministerie van defensie. Het programma "Informatiebeveiliging" is een sterke randvoorwaarde voor de informatievoorziening van Defensie.

DEFENSIE BEVEILIGINGSBELEID

Het beleid op het gebied van informatiebeveiliging is bij het Ministerie van Defensie vastgelegd in het Defensie BeveiligingsBeleid (DBB). Dit Beveiligingsbeleid is gebaseerd op de vigerende internationale en nationale wet- en regelgeving. Het DBB bevat het beveiligingskader, waarbinnen systematisch en vergelijkbaar met alle aspecten van beveiliging wordt omgegaan. Het DBB beschrijft de specifieke kaders voor informatiebeveiliging en de beveiliging van materieel en personeel. Dit DBB dient te worden beschouwd als een noodzakelijke tussenschakel naar een compleet en volledig geïntegreerd beveiligingsbeleid. Dit beleid is op 13 augustus 1997 vastgesteld door de Secretaris-Generaal en van kracht verklaard voor de beleidsterreinen.

Het informatiebeveiligingsbeleid is een verzameling strategische uitgangspunten waarin het topmanagement van defensie het tactisch en operationeel niveau duidelijk maakt welke gedragslijn defensie aanneemt om te komen tot een afgewogen stelsel van maatregelen.

Op strategisch niveau vindt beleidsformulering plaats, op tactisch niveau wordt dit beleid vertaald naar concreet te treffen maatregelen die op operationeel niveau worden uitgevoerd. Op alle niveaus vindt controle en evaluatie plaats (zie figuur 1).

Controle houdt in: "het vaststellen of de beoogde taken en maatregelen adequaat worden uitgevoerd". Evaluatie houdt in: "het vaststellen of het beoogde samenstel van verantwoordelijkheden, taken en bevoegdheden, alsmede de maatregelen op zich nog steeds effectief zijn in het licht van de te behalen beveiligingsdoelstellingen". Het beveiligingsbeleid (inclusief informatiebeveiliging) staat onder invloed van zowel politieke, maatschappelijke als technische ontwikkelingen. Periodieke evaluatie en zonodig aanpassing van het beveiligingsbeleid is daarom geboden. De input voor deze evaluatie is het resultaat van de beoordeling van het DBB op toereikendheid, die wordt uitgevoerd door de onafhankelijke deskundige de DEFAC. Het DBB is momenteel in evaluatie bij de Beveiligingsautoriteit. Het Defensie Beveiligingsbeleid is gepubliceerd op het intranet van Defensie en te vinden op de website van de Centrale Organisatie (http://www.navy.mindef.nl/co/beveiliging/).

PROGRAMMA INFORMATIEBEVEILIGING

De doelstelling van informatiebeveiliging is de waarborging van een betrouwbare informatievoorziening. Het doel van het programma informatiebeveiliging is het op een beheersbare wijze

Figuur 1: Proces informatiebeveiliging

realiseren van een adequate beveiliging conform het Voorschrift Informatiebeveiliging Rijksdienst en de verwerving van defensiebrede technische informatie beveiligingsproducten.

Doelstellingen VIR

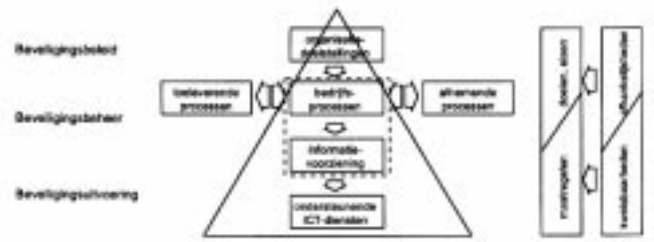
Op het pad naar het einddoel, waarbij informatiesystemen en verantwoordelijkheidsgebieden van Defensie volledig aan het VIR voldoen, zijn mijlpalen vastgesteld. Deze, door de IVR in november 1999, vastgestelde mijlpalen zijn:

- 1 april 2000: voor elk vitaal informatiesysteem en verantwoordelijkheidsgebied een vastgesteld informatiebeveiligingsplan.
- 1 januari 2001: voor 50 % van de informatiesystemen en verantwoordelijkheidsgebieden een vastgesteld informatiebeveiligingsplan.
- 1 januari 2002: voor 75 % van de informatiesystemen en verantwoordelijkheidsgebieden een vastgesteld informatiebeveiligingsplan.
- 1 juli 2002: voor elk informatiesysteem en verantwoordelijkheidsgebied een vastgesteld, geïmplementeerd en goedgekeurd informatiebeveiligingsplan.

Alle beleidsterreinen zijn momenteel met zeer veel inspanning bezig de mijlpalen, die gesteld zijn op 1 januari 2002 en 1 juli 2002 te realiseren. Verwacht wordt dat alle beveiligingsplannen zijn vastgesteld, de belangrijkste maatregelen zijn geïmplementeerd, de uitvoering van de overige maatregelen zijn gepland en het restrisico door de verantwoordelijken is geaccepteerd. In aanvulling op bovengenoemde mijlpalen heeft het Politiek Beraad (PB komt al voor in voorwoord) op 16 augustus 2000 ingestemd met de invoering van het basisbeveiligingsniveau (de Defensiebaseline in VIR: gemeenschappelijke betrouwbaarheidseisen) voor de standaard ICT-infrastructuur van Defensie in 2001.

Het VIR

Bedrijfsprocessen in organisaties zijn in belangrijke mate afhankelijk van goed functionerende informatiesystemen. Veel processen zijn nagenoeg onmogelijk zonder de toepassing van geautomatiseerde gegevensverwerking. Uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden, of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de beleids- en bedrijfsvoering. Een afdoende beveiliging van gegevens is derhalve noodzakelijk (zie figuur 2).



Figuur 2: Afhankelijkheid, kwetsbaarheid

In het Defensie Beveiligingsbeleid (gebaseerd op het Voorschrift Informatiebeveiliging Rijksdienst (VIR94)) is aangegeven dat voor ieder informatiesysteem en verantwoordelijkheidsgebied door de verantwoordelijke commandant een afhankelijkheids- en kwetsbaarheidsanalyse dient te worden uitgevoerd. De uitwerking hiervan is in een andere bijdrage in deze Intercom weergegeven. Het resultaat van deze analyse geeft inzicht in de mate waarin bedrijfsprocessen afhankelijk zijn van o.a. het adequaat functioneren van het informatiesysteem, alsmede een set van betrouwbaarheidseisen die aan het informatiesysteem of verantwoordelijkheidsgebied worden gesteld.
Aan de hand van de vastgestelde betrouwbaarheidseisen en rekening houdend met de systeem specifieke dreiging dient het te treffen stelsel van beveiligingsmaatregelen te worden bepaald. Voor ieder informatiesysteem of verantwoordelijkheidsgebied dienen door de verantwoordelijke commandant de te nemen beveiligingsmaatregelen in een informatiebeveiligingsplan te zijn vastgelegd. Het stelsel omvat maatregelen van organisatorische, procedurele, fysieke (bouwkundig / bewaking) en technische (indringer detectie / hardware / software) aard. Het gehele stelsel van maatregelen wordt in het programma informatiebeveiliging behandeld onder het onderwerp “VIR”. Daarnaast is binnen het programma bijzondere aandacht voor informatiebeveiligingsmiddelen die bruikbaar zijn als (deel van) beveiligingsmaatregelen.

In het Defensie Beveiligingsbeleid is aangegeven dat (om de taak van de commandant te verlichten) op centraal niveau een Baseline van Gemeenschappelijke Betrouwbaarheidseisen worden vastgesteld in de vorm van een set van betrouwbaarheidsniveaus. Een betrouwbaarheidsniveau bevat alle betrouwbaarheidseisen, die voor een de desbetreffende situatie gelden. De betrouwbaarheidseisen bevatten een combinatie van eisen voor zowel de exclusiviteit (vertrouwelijkheid), integriteit als beschikbaarheid.

Aangezien informatiesystemen en verantwoordelijkheidsgebieden veelal gebruik maken van een identieke Informatie en Communicatie Technologie (ICT)-omgeving kunnen ook de beveiligingsmaatregelen op een zelfde wijze worden geïmplementeerd. De taak van de commandant om een beveiligingsplan op te stellen en te implementeren wordt met de beveiligingsniveaus en standaard ICT-infrastructuur in belangrijke mate verlicht.
Met de implementatie van de baseline is het mogelijk defensie breed vertrouwelijke niet gerubriceerde informatie uit te wisselen. Uitwerking hiervan zal in een ander bijdrage in dit blad worden toegelicht.

HET TECHNISCH INFORMATIEBEVEILIGINGS INITIATIEF: TIBI

Voordat er nog maar op enigerlei wijze sprake was van programmamanagement in de zin zoals hiervoor beschreven, had “de overheid” het initiatief genomen de beveiliging van de informatievoorziening op een (veel) hoger plan te brengen. In de voormalige Nationale Verbindingsbeveiligings Raad (NVBR) was met inbreng van o.a. Defensie en TNO/FEL de architectuur voor beveiliging van bijzondere informatie ontworpen, de zgn. Staatsgeheime informatie. De kern hiervan werd gevormd door een cryptografisch hart met daaromheen zelfontwikkelde software voor de besturing in een standaard personal computer.
Deze ontwikkeling is het technisch informatiebeveiligingsinitiatief (TIBI). De realisatie van dit TIBI is als overheidsinitiatief gestart in 1995 met een haalbaarheidsonderzoek. Uit dit onderzoek, dat in samenwerking met de nationale crypto-industrie Philips Crypto BV en het Nationaal Bureau voor Verbindingsbeveiliging (NBV) was opgestart, bleek dat het mogelijk zou zijn computerbeveiligingsmaatregelen te ontwikkelen op basis van het Microsoft besturingssysteem NT 4 en een speciale hardware module die vercijfering van bestanden mogelijk moet maken tot het niveau “Staatsgeheim Geheim”. Bovendien wordt sterke authenticatie toepast met een smartcard. Deze speciale hardwaremodule was de zgn. vercijferkaart (V-kaart). Dit betekent dat een hoog niveau van vertrouwelijkheid haalbaar zou zijn, veel hoger dan met commerciële middelen. Voor de bijbehorende netwerkbeveiliging was een virtual private network guard (VPN-Guard) voorzien. Het cryptosleutelmanagement, dat noodzakelijk is om transport en beheer van cryptosleutels mogelijk te

maken, zou op basis van een Key Distribution Centre (KDC) en een Credentials Distribution Centre (CDC) worden uitgevoerd. De basis voor zo'n KDC/CDC is een public key infrastructure (PKI/TTP) met daarin geïntegreerd de on-line distributie en registratie van cryptosleutelmateriaal.

Medio 1997 is het contract voor de ontwikkeling van de V-kaart gesloten en in november het contract voor de VPN-Guard. De ontwikkeling V-kaart, te beginnen met het ontwikkelen van de speciale cryptomodule en vervolgens de softwarematige integratie in Windows NT, zou twee jaar in beslag nemen en zou in twee stappen (versie 1 voor stand-alone pc's, en versie 2 voor pc's in netwerken en voor de VPN-Guard) worden uitgevoerd. Nadat echter bleek dat de praktijk toch weerbarstiger was dan de theorie, werd de ontwikkeling verlengd met nog een jaar. Ook na deze verlenging bleek het niet mogelijk een stabiel werkend V-kaartsysteem op te leveren. Het diep ingrijpen in de code van Windows bleek onvoorspelbaar gedrag op te leveren doordat de broncode (sourcecode) en daarmee dus de diepere logica in Windows niet beschikbaar was. Nu was goede raad duur. Na overleg met de leverancier is besloten de eisen voor het V-kaartsysteem te wijzigen. Er zou een versie ontwikkeld worden die alleen geschikt zou zijn voor gebruik in stand-alone computers. De netwerkversie zou in een later stadium verder ontwikkeld worden.
Omdat de ontwikkeling VPN-Guard in hoge mate afhankelijk was van netwerkfunctionaliteit van de V-kaart, kon de VPN-Guard ook niet voltooid worden. Het is gebleven bij een netwerksysteem dat vergelijkbaar is met producten van andere leveranciers. Er zat dus geen toegevoegde waarde in de ontwikkeling van deze VPN-Guard voor Staatsgeheime informatie.

Nadat vervolgens de fabriekstesten met de V-kaart ("doet hij wat hij moet doen") succesvol waren verlopen, werd een uitgebreide praktijktest (pilot) gehouden met "life" gebruikers. Vervolgens evalueerde het Nationaal Bureau voor Verbindingsbeveiliging (NBV) het functioneren van de cryptografische kern van de V-kaart en de aansturing daarvan door de beveiligingssoftware en testte TNO/FEL de betrouwbaarheid van de gehele computer met geïnstalleerde V-kaart. Deze testen van TNO/FEL waren vooral gericht op de inbraakgevoeligheid van de kaart ("doet hij niet wat hij niet moet doen"). De praktijktesten bevestigden de bevindingen van het NBV en TNO/FEL dat de V-kaart niet aan de (hoge) verwachtingen voldeed. Vervolgens is onderzocht of de V-kaart zodanig aangepast kon worden dat deze alsnog aan de gestelde zware beveiligingseisen zou voldoen. Dit zou volgens alle betrokken partijen een enorme technische en dus dure inspanning vereisen, waarbij succes niet was gegarandeerd. Vervolgens is besloten het ontwikkeltraject V-kaart te stoppen. Het deelproject voor cryptosleutelmanagement was ondertussen gestart met een uitgebreide pilot met alle krijgsmachtdelen voor het testen van het gebruik en het beheer van een commerciële public key infrastructure (PKI) in de bedrijfsnetwerken zoals LAN2000. Deze pilot was uitermate goed geslaagd bij gebruikers en bij de beheersorganisatie van DTO. Over dit projectdeel is in deze uitgave van Intercom nog een speciaal artikel opgenomen. Omdat ondertussen de V-kaart was mislukt, werd ook het cryptodistributie mechanisme niet in ontwikkeling genomen. En zo is aan een toch zeer ambitieus programma voor informatiebeveiliging een einde gekomen.

LESSONS LEARNED

Wat hebben we nu geleerd van het mislukken van de V-kaart?

- In de eerste plaats was de integratie met de bestaande IV ontwikkelingen niet adequaat. Het project LAN2000, dat later was gestart dan de V-kaart en gebaseerd was op diverse netwerkontwikkelingen en centraal beheer, kon i.v.m. de Millenniumopdracht niet wachten op de reeds vertraagde ontwikkeling van de V-kaart. Bovendien verdroeg dit centraal beheer zich niet met de gedachte achter de V-kaart dat een niet-sterke authenticatie van de op afstand opererende beheerder de veiligheidsmaatregelen van de V-kaart zou omzeilen.
  o Les: ... eisen vaststellen en daarna snel komen tot een eerste versie van het product.
- Ten tweede is de ontwikkeling van eigen speciale beveiligingssoftware zeer moeilijk gebleken omdat van het gebruikte computerbesturingssysteem geen broncode beschikbaar was en het besturingssysteem derhalve een blackbox is. Ingrijpen in de besturing zonder gebruik te maken van de beschikbare application programming interfaces (API's) was dus onmogelijk. Vanwege de hoge vereiste betrouwbaarheid kon van deze API's dan ook geen gebruik gemaakt worden.
  o Les: ... gebruik evalueerbare (gedocumenteerde) systeemsoftware i.c. besturingssystemen.
- Op de derde plaats was de opstap van "niets c.q. weinig" naar "geheim" een te grote technische en daarmee zeer risicovolle stap. Wanneer eerst evolutionaire ontwikkelingen voor sensitieve, dus niet staatsgeheime informatie hadden plaatsgevonden dan was het risico waarschijnlijk kleiner geweest en had men beter kunnen leren van deze eenvoudiger ontwikkeling. Het vernieuwde beveiligingsbeleid heeft daar terecht op ingespeeld door alsnog te beginnen met commerciële producten voor het basisbeveiligingsniveau.
  o Les: ... beperken van het ambitieniveau, ontwikkelen in kleine stappen (evolutionair in plaats van revolutionair).
- Ten vierde was het traject voor certificering bij aanvang van het project niet helder gedefinieerd. Dit heeft geleid tot het stap-voor-stap ontwikkelen van die zware betrouwbaarheidseisen. Bovendien was de normering volgens Common Criteria (CC), de ITU standaard voor informatiebeveiliging, nog niet geheel "tussen de oren" van de kwaliteitsborgers. De voorgaande Europese standaard ITSEC werd na 1996 vervangen door CC versie 1 en in 1999 door versie 2 die natuurlijk afweek van de voorgaande. Dit "inleren" vooral op CC versie 2 heeft enorm veel kennis opgeleverd die nu ten goede komt aan de Nederlandse overheid. Juist één van de doelstellingen van het project VPN-Guard was het vertalen van de algemene CC naar een handzaam en werkbaar instrumentarium. In dit opzicht is TIBI zeer opbouwend geweest voor het toepassen van maatregelen voor informatiebeveiliging.
  o Les: ... eisen voor evaluatie in het contract "programma van eisen" meetbaar vastleggen en hieraan vasthouden.

Het juist interpreteren van kwaliteitseisen voor de informatievoorziening en de toepassing daarvan in combinatie met een afgewogen oordeel over veiligheidsrisico´s is van groot belang voor de uitvoering van het VIR, niet alleen voor Defensie maar ook voor andere overheden en de industrie. Ondank het niet slagen van het V-kaart project in engere zin, is de overheid er toch in geslaagd de geleerde lessen toe te passen en de kennis opgedaan met deze projecten te benutten voor toekomstige ontwikkelingen, zowel bij de behoeftestellers, de verwervers, de kwaliteitsborgers als de certificeerders. ■