NETWERK EN INFORMATIE INFRASTRUCTUUR

STRATEGISCHE VISIE

De HDIO en CDS hebben eind 2011 gezamenlijk een strategische visie op de Netwerk en Informatie Infrastructuur (NII) gepubliceerd. In de visie is het streefbeeld beschreven dat Defensie beschikt over één NII voor de ondersteuning van alle operationele, ondersteunende en bestuurlijke processen, die centraal wordt beheerd en waarover beveiligde data kan worden uitgewisseld met samenwerkende militaire en niet-militaire partners onder alle gebruiksomstandigheden. In één zin samengevat: De NII maakt genetwerkt samenwerken mogelijk. In dit artikel, dat met medewerking van lkol ir. Jan van de Pol (namens de HDIO) tot stand is gekomen, een integrale weergave van deze strategische visie.

INLEIDING

"De traditionele dimensies van de operatiegebieden zee, land en lucht, worden uitgebreid met de dimensies ruimte en informatie (waaronder cyber)." *(Bron: MSV 2010)*

In de Militair Strategische Visie (MSV) 2010 geeft de CDS aan dat netwerkend optreden essentieel is voor de militair. Het is van belang om te realiseren dat de militair centraal staat, en dat *Network Enabled Capabilities* (NEC) hem ondersteunen om zowel nationaal, internationaal, militair en civiel op te treden en samen te werken. In termen van informatievoorziening (IV) staat Defensie voor de volgende uitdaging:

"Altijd en overal, veilige, geautoriseerde toegang tot de juiste en volledige informatie, nodig voor een doeltreffend functioneren." *(Bron: HDIO, IV-Strategie "IV4ALL", 2010)*

Om dit te bereiken is een toereikende, toekomstvaste en structureel betaalbare ICT-infrastructuur essentieel. Binnen NAVO wordt, voor de realisatie van NEC, gesproken over een samenhangende Netwerk en Informatie Infrastructuur (NII). Voorliggende strategische visie schetst een beeld van de huidige situatie en geeft richting aan de ondersteuning van de nieuwe dimensies van militair optreden met een NII, niet alleen in een operationele maar ook in de bestuurlijke omgeving.

DEFINITIE

Voor de scope en reikwijdte van deze strategische visie sluiten we aan bij de NAVO definitie waarin de NII bestaat uit de volgende NAVO NEC capaciteiten: Communicatie, Integratie van Informatie, Informatiebeveiliging en Service Management Control.

De traditionele Defensie ICT-infrastructuur beperkt zich daarbinnen voornamelijk tot de capaciteit Communicatie. De capaciteiten Gebruikers & Taakgebieden en Samenwerkingsverbanden & Functionele Diensten maken weliswaar geen deel uit van de definitie maar moeten wel worden bezien in relatie met de NII.

De NII omvat alle voorzieningen om informatie door middel van communicatie en informatie integratie te verwerken, te delen, te presenteren, te beveiligen en het geheel te beheren. (T.o.v. de traditionele (hardware georiënteerde) ICT-infrastructuur betekent dit een verbreding van de scope met generieke IV-diensten voor de ondersteuning van samenwerkingsverbanden). Het publieke internet vormt tegenwoordig als informatiebron en als informatiesnelweg een onmisbaar onderdeel van deze infrastructuur.

NAVO NEC capaciteiten

SITUATIESCHETS

Interoperabiliteit

Commandanten ervaren tijdens operationele inzet dat de effectiviteit van het optreden te kort schiet als gevolg van gebrek aan interoperabiliteit tussen de verschillende samenwerkende partijen. Interoperabiliteit moet op verschillende niveaus (organisatie, processen, informatie en techniek) worden gerealiseerd maar is in belangrijke mate afhankelijk van de beschikbaarheid van 'gesloten' communicatiekanalen en netwerken. Nu brengen alle partijen nog hun eigen systemen mee die niet of moeizaam kunnen worden gekoppeld. Hierdoor kunnen mensen elkaar niet bereiken en er kan geen digitale informatie snel en eenvoudig worden uitgewisseld. Er vallen zelfs onnodig slachtoffers als de informatie over posities en plannen van eigen en vijandelijke troepen niet juist en tijdig beschikbaar is. Vooral de samenwerking met niet-militaire partijen, andere (overheids)organisaties en ook de industrie, blijkt moeizaam te verlopen vanwege het gesloten karakter van defensieorganisaties en infrastructuur.

Beschikbaarheid

Binnen Defensie wordt traditioneel een onderscheid gemaakt tussen de informatievoorziening ten behoeve van operationele, ondersteunende en bestuurlijke processen. In veel gevallen heeft dit ertoe geleid dat er verschillende, van elkaar gescheiden, ICT-infrastructuren ('stovepipes') zijn ontstaan mede op basis van rubriceringen en gebruiksomstandigheden. Procesgrenzen vervagen echter als bijvoorbeeld, sneller dan in de publieke media, nut en noodzaak van militaire acties op het laagste (uitgestegen) niveau moeten worden verantwoord aan de politieke leiding in de statische omgeving

(maatschappelijke relevatie). Andersom is er in het operatiegebied behoefte aan informatie uit de ondersteunende en bestuurlijke systemen om de eenheden in staat te stellen hun taak uit te laten voeren. Defensie moet daarom kunnen beschikken over gesloten en betrouwbare informatieketens tussen de uitgestegen, mobiele, ontplooide en statische gebruiksomstandigheden. Beschikbaarheid in termen van 'Any time, any place, any device' (*Bron: HDIO, IV4ALL, 2010*) wordt nu niet gehaald omdat de netwerken en informatiesystemen er (nog) niet op zijn ingericht, maar is wel de ambitie.

Betaalbaarheid
De grote hoeveelheid transmissiesystemen en netwerken die zijn ontstaan binnen Defensie worden dagelijks door een groot aantal professionals in stand gehouden. Door versnippering en legacy is steeds meer budget nodig en op langere termijn leidt dit onherroepelijk tot problemen. Systemen bereiken vaak uit fase het einde van de levensduur en worden meestal nog, op traditionele wijze, één-op-één vervangen op basis van een investeringsafweging. In veel gevallen is zelfs niet bekend hoe groot de daadwerkelijke exploitatie is. In het belang van een samenhangende NII moeten keuzes gemaakt worden op basis van de integrale kosten (*Total Cost of Ownership*) van het totale systeemlandschap (NII-portfolio).

Internet
Vanuit beveiligingsoptiek wordt doorgaans zeer terughoudend omgegaan met het gebruik van het internet voor defensiedoeleinden. Internet wordt echter in toenemende mate een belangrijke informatiebron voor Defensie en in veel gevallen is internet het enige (transmissie)medium waarover andere, niet-militaire partijen beschikken om met Defensie informatie uit te wisselen.

Toekomstvastheid
De hoeveelheid digitale informatie stijgt, o.a. door het toenemend gebruik van sensoren, exponentieel en stelt daarmee steeds hogere eisen aan de netwerken en transmissiesystemen op het gebied van (wereldwijde) dekking en benodigde bandbreedte. Deze capaciteiten moeten daarom flexibel kunnen meegroeien met de vraag. In dit kader speelt het belang van *reach-back* capaciteit voor het verkleinen van de expeditionaire footprint een belangrijke rol. Niet alleen voor het efficiënt benutten van schaarse capaciteit in de inlichtingenketen of het op afstand plaatsen van staven maar ook voor het beheer en onderhoud van systemen op afstand. Defensie maakt onvoldoende gebruik van de winst die gehaald kan worden uit het op afstand aanbieden van opleidingen en trainingen (*eLearning*) en de mogelijkheden die ontstaan met het koppelen van trainers, simulatoren en eenheden over de netwerkinfrastructuur. Ook hierbij spelen betere connectiviteit en meer bandbreedte een essentiële rol. In dit kader moet ook gedacht worden aan het aanbieden van opleidingen op en over het internet.

Het Nieuwe Werken
Defensie wordt geconfronteerd met een nieuwe generatie 'informatiewerkers' die opgroeit met internet en mobiele apparaten die volop mogelijkheden bieden voor 'self-empowerment', 'Social Community Networking' en 'Unified Communications'. Deze nieuwe informatietechnologie ondersteunt Het Nieuwe Werken (HNW) waarin mensen en organisaties flexibeler omgaan met arbeidstijd en werkomgeving. Werving en behoud van personeel is sterk afhankelijk van de mate waarin Defensie HNW kan (gaan) ondersteunen in de infrastructuur. Met de mogelijkheden voor effectiever, plaats- en tijdonafhankelijk werken vormt HNW tevens een potentiële bron voor besparingen.

OPERATIE ATALANTA
In EU verband werd tijdens de operatie ATALANTA gekozen voor het gebruik van beveiligde voorzieningen op internet. Enerzijds om te voorzien in een niet bestaand EU communicatiesysteem, anderzijds om een NII mogelijk te maken voor een ongekend divers samenwerkingsverband (met daarin o.a. NAVO, EU, CHIN, KSA, Civiele scheepvaart, RUS, JAP, AUS, ROK, SEY, etc).

PROBLEEMSTELLING
De huidige Netwerk en Informatie Infrastructuur van Defensie:
- voldoet niet aan de eisen en wensen op het gebied van interoperabiliteit, beschikbaarheid, betaalbaarheid;
- maakt nog maar beperkt gebruik van internet als informatiebron en als transmissiemedium;
- is niet toekomstvast voor wat betreft de toenemende behoeftes aan bandbreedte, opslag- en verwerkingscapaciteit voor onder andere sensordata, reach-back en O&T voorzieningen;
- is niet berekend op gelegenheidscoalities;
- is niet berekend op de nieuwe generatie medewerkers en 'Het Nieuwe Werken'.

STRATEGISCHE RICHTLIJNEN
De NII, zoals in deze visie beschreven, levert een belangrijke bijdrage aan de ontwikkeling van (elementen van) de zeven samenhangende Essentiële Operationele Capaciteiten of kortweg EOC'n uit de MSV 2010.
- EOC1 Tijdige beschikbaarheid:
  - ✓ "Optimaal gebruik maken van schaarse onderwijsleermiddelen"
  - ✓ "Levensechte simulatie maakt oplei-ding en training realistischer en doelmatiger"
- EOC2 Gevalideerde inlichtingen:
  - ✓ "Inlichtingen en informatie zijn de motor voor besluitvorming"
  - ✓ "De verspreiding van inlichtingen binnen een gezamenlijke, geïntegreerde en genetwerkte omgeving moet zorgen voor opbouw van een gemeenschappelijk omgevingsbeeld dat tot op het laagste niveau verspreid moet kunnen worden"
  - ✓ "De informatie dimensie is niet alleen een bron maar ook een dreiging (cyber aanvallen) die specifieke inlichtingenexpertise vereist"
- EOC3 Ontplooibaarheid en mobiliteit:
  - ✓ "Om de belasting van strategische transportcapaciteit te verminderen moet de expeditionaire footprint in omvang en gewicht zo klein mogelijk zijn"
- EOC4 Effectieve inzet:
  - ✓ "Bij huidige en toekomstige operaties zijn informatieoperaties en civiel-militaire samenwerking kernonderdelen van de militaire inspanning"
- EOC5 Hoogwaardige commandovoering:
  - ✓ "Voor een hoogwaardige commandovoering streven we naar informatiedominantie"
  - ✓ "In een NEC-omgeving worden sensoren, effectbrengers en commandovoerings-elementen bijeengebracht"
  - ✓ "Reach-back, in de vorm van commandovoering ondersteuning op afstand, verkleint de footprint in het inzetgebied en zorgt voor (indirecte) bescherming"
- EOC6 Adequate logistieke ondersteuning:
  - ✓ "Kwetsbaarheid verlagen door te streven naar een kleinere logistieke footprint ter plekke…"
  - ✓ "Optimale besturing van de joint logistieke processen door robuuste automatisering"
- EOC7 Veiligheid en bescherming:
  - ✓ "Ook het maximaal gebruik maken van reach-back faciliteiten is een vorm van bescherming"
  - ✓ "Geautomatiseerde locatiebepaling en identificatie van de eigen eenheden is essentieel om de kans op 'broedermoord' te minimaliseren"
  - ✓ "De toenemende afhankelijkheid van automatisering in een genetwerkte omgeving vereist bescherming tegen een cyberaanval door tegenstanders"

Alle EOC'n zijn dus afhankelijk van een toereikende, toekomstvaste en betaalbare NII die de basis vormt voor effectief en efficiënt optreden, onafhankelijk van de specifieke inrichting van de krijgsmacht. Voor de ontwikkeling en realisatie van de NII is het

noodzakelijk om op strategisch niveau richtinggevende principes overeen te komen op het gebied van:

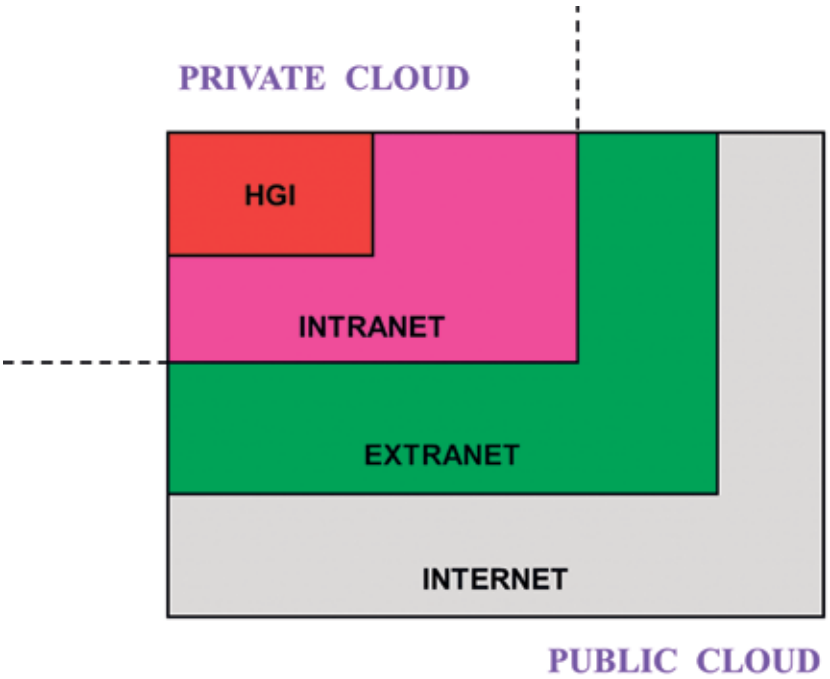
- Netwerken, beveiliging en beheer,
- Interoperabiliteit en standaardisatie,
- *Sourcing en partnership*,
- Planning, realisatie en innovatie,
- Personeel, opleiding en training.

RICHTINGGEVENDE PRINCIPES

Netwerken, beveiliging en beheer

Defensie kent nu nog vele netwerken en transmissiesystemen die niet gekoppeld zijn dan wel niet gekoppeld mogen of kunnen worden vanuit informatiebeveiliging- of beheeroptiek. Gesloten communicatiekanalen over netwerken en transmissiesystemen vormen de basis voor het snel en veilig kunnen uitwisselen van informatie over grote afstanden. Voor de operator (verzamelbegrip voor alle (eind)gebruikers van de NII van de 'Warfighter' tot en met de 'bestuurder') moet het er niet toe doen hoe dit achter de 'stekker' (bij voorkeur één) is ingericht. Het moet dan ook mogelijk zijn om vanaf dezelfde computer (laptop) op een willekeurige werklocatie (op kantoor of in het veld) gebruik te maken van zowel de operationele als de ondersteunende en de bestuurlijke systemen. Achter de schermen moet de gewenste toegang en afhankelijk van de gebruiksomstandigheden de vereiste mate van continuïteit en overleefbaarheid kunnen worden gegarandeerd en zal bij degradatie van het netwerk voorrang moeten worden verleend aan de ondersteuning van de meest essentiële taken.

In nationale en internationale staven zijn meerdere netwerken beschikbaar om te voldoen aan verschillende beveiligingsniveaus en de bescherming van de verschillende nationale belangen (rubriceringen). Als stip op de horizon moet Defensie streven naar één 'black core' met daarop beveiligde data. Dit maakt het gebruik van verschillende netwerken voor de verschillende vertrouwelijkheidsniveaus overbodig. Zolang de techniek voor het beveiligen van dataobjecten nog niet voorhanden is, moeten beveiligingsoplossingen worden gevonden voor het rationaliseren van de grote hoeveelheid bestaande, fysiek gescheiden hoog gerubriceerde netwerken naar één Hoog Gerubriceerd Informatiedomein (HGI). Daarbuiten moet informatie laagdrempelig, op eenvoudige en intuïtieve wijze, kunnen worden gedeeld in de verschillende samenwerkingsverbanden. Vooralsnog hanteert Defensie echter een vrij rigide scheiding tussen het interne netwerk (intranet) en de externe omgeving (internet).



Schematische indeling van de Public Cloud en de Private Cloud

Afhankelijk van de mate van vertrouwelijkheid bestaat er voor de communicatie met externe partijen en de industrie behoefte aan meer transparante koppelingen met het internet. Bij veilige koppelingen spreken we vaak over een extranet waarover Defensie informatie en diensten kan uitwisselen met externe partners. De meest recente IT-ontwikkelingen zijn gericht op het leveren van IV en ICT functies in de vorm van diensten (services) vanuit een zogenaamde 'public cloud', een voor iedereen beschikbaar domein zoals het internet. Als dezelfde technologie op het intranet wordt toegepast spreken we over een 'private cloud'. Het is van belang om vast te stellen welke partijen in bestaande en nog te verwachten samenwerkingsverbanden deel uitmaken van één of meer van deze informatiedomeinen. Vervolgens moet bepaald worden welke beveiligingsmaatregelen nodig zijn op de verschillende koppelvlakken. Deze benadering maakt het verlenen en afnemen van IT-diensten (SaaS, PaaS en IaaS; vrij vertaald: 'software als een dienst', 'datacenters als een dienst' en 'infrastructuur als een dienst') mogelijk wat leidt tot een betere samenwerking tegen lagere kosten.

De basis voor technische oplossingen op het gebied van informatiebeveiliging wordt gelegd met de inrichting van *Identity* en *Access Management* (IAM) op basis van een vertrouwde *Public Key Infrastructure* (PKI). Daarbij dient ook aandacht te worden besteed aan het verlenen van autorisaties aan ketenpartners waaronder andere (overheids) organisaties maar ook de industrie (zoals bijvoorbeeld in het *Trans global Secure Collaboration Program* (TSCP). Risicomanagement dient vervolgens een bijdrage te leveren aan een welbewuste keuze tussen openheid en veiligheid). Bovendien moet meer dan voorheen het tijdelijke karakter van gerubriceerde informatie meewegen in de oplossingen. Kennis van (technische) beveiligingsoplossingen is een nationale aangelegenheid. Defensie moet kunnen beschikken over stafcapaciteit voor kennisopbouw, met name op het gebied van beveiligingsstandaarden en accreditatie van IT-diensten. Informatiebeveiliging moet vroegtijdig worden meegenomen in het behoeftestellingsproces (DMP) en het Operationele Planningsproces (OPP). Het beveiligingsbewustzijn van de operators dient waar mogelijk verder te worden ontwikkeld.

Vanuit beheer (NNEC: *Service Management Control*) optiek hebben we te maken met het naast elkaar gebruiken van verschillende beheerconcepten die voortkomen uit de informatievoorziening, het wapensysteemmanagement, de materieellogistiek, de telecommunicatie en de datacommunicatie. Deze verschillen weliswaar niet fundamenteel van elkaar maar moeten qua terminologie, begrippen en in het bijzonder voor wat betreft werking op elkaar worden afgestemd. Verschillende organisatorische, geografische en technische inrichtingen van beheer(omgevingen) vormen niet alleen intern Defensie, maar zeker ook internationaal, een belemmering voor interoperabiliteit en samenwerking.

Een voorbeeld van een nieuwe NII is de inrichting van het *Afghan Mission Network* (AMN) door NAVO, waarbij nationale (militaire) netwerken gekoppeld worden aan een centraal beheerd 'core' netwerk. Bij de realisatie is gekozen voor samenwerking met

de industrie die de uitrol in Afghanistan heeft gedaan. De werking en het succes van een dergelijke aanpak is sterk afhankelijk van het op hoog niveau afdwingen van standaarden en wederzijds vertrouwen: 'aansluiten en meedoen om informatie met elkaar te kunnen delen'. Essentieel is de bereidheid tot het delen van informatie op één beveiligingsniveau met alle betrokken partijen. Tevens blijkt dat een gesloten en betrouwbare informatieketen over verschillende samenwerkende partijen heen momenteel alleen haalbaar is als beheerconcepten, –processen, –procedures en –inrichting dezelfde zijn of op elkaar zijn afgestemd. Vooralsnog is het samenbrengen van de beheerorganisaties, zowel intern Defensie als met die van partners in het operationele optreden, randvoorwaardelijk voor het sluiten van de informatieketen.

De toenemende afhankelijkheid van informatie infrastructuren leidt tot een nieuwe bedreiging. Aanvallen op netwerken met als doel informatie te vergaren en/of systemen onbruikbaar te maken (cyberwarfare) vereisen het nemen van maatregelen. Het geheel van defensieve maatregelen wordt samengevat onder het begrip cyberdefence. De effectiviteit van cyberdefence neemt toe bij een afnemend aantal systemen (ultimo één) die beheerd worden vanuit een centraal *Network Control Center*. Keerzijde hiervan is echter weer een toenemende kwetsbaarheid. De oplossing hiervoor moet gevonden worden in het aanbrengen van redundantie binnen de netwerken maar ook in diversiteit waaronder een uitgebalanceerde mix van militaire en civiele capaciteiten.

In het kader van ontplooibaarheid en mobiliteit (EOC3) moet de NII voldoende capaciteit bieden voor *reach-back* om de expeditionaire footprint te minimaliseren. Wereldwijde inzetbaarheid betekent vervolgens ook dat Defensie te allen tijde moet kunnen beschikken over mondiale satellietcapaciteit. Vanuit effectiviteit en efficiëntie overwegingen moet een balans gevonden worden tussen dure, betrouwbare militaire bandbreedte en beschikbare civiele capaciteiten. Voor het geval satellietcapaciteit (tijdelijk) een bottleneck vormt in de IV-keten zal de kwaliteit van essentiële informatiestromen of diensten (*Quality of Service*) gewaarborgd moeten blijven. Omdat satellietverbindingen kunnen uitvallen, of alle communicatiemiddelen bewust kunnen worden uitgezet, moet in alle operationele, ondersteunende en bestuurlijke systemen het decentrale server concept worden toegepast voor het behoud van autonomiteit in de *deployed* omgeving.

Strategische richtlijnen:

- Defensie richt, vanuit het gebruikersperspectief, één (federatief) netwerk in voor alle operationele, ondersteunende en bestuurlijke processen.
- Voor de inrichting van de werkplek (computer) geldt als uitgangspunt (eventueel gelijktijdige) toegang tot operationele, ondersteunende en bestuurlijke systemen.
- Defensie streeft één netwerk na met daarop beveiligde data. (NB: Ultiem *Multi Level Secure* (MLS) maar *black core* dat is technisch voorlopig nog niet mogelijk.)
- Defensie realiseert vooralsnog één Hoog Gerubriceerd Informatiedomein.
- Defensie moet zelf beschikken of kennis op gebied van informatiebeveiliging, inclusief standaarden en accreditatie.
- Defensie moet onder alle omstandigheden kunnen beschikken over (bij voorkeur veilige) toegang tot internet.
- Defensie houdt zelf de regie in handen op het gebied van de architectuur van de NII.
- Defensie gaat, meer dan nu in de praktijk het geval is, over van het vermijden van risico's naar het bewust accepteren en managen van risico's.
- Gerubriceerde data moet te allen tijde kunnen worden voorzien van een 'houdbaarheidsdatum'.
- Defensie deelt informatie uitsluitend op basis van gecontroleerde en geautoriseerde toegang.
- Het beheer van de NII wordt centraal geregisseerd en ingericht.
- De Defensie NII heeft in het kader van wereldwijd optreden behoefte aan satellietcapaciteit voor *reach-back*.
- De benodigde satellietcapaciteit wordt geborgd in een uitgebalanceerde mix van militaire en commerciële systemen.
- Satellietcapaciteit is een integraal onderdeel van de NII.
- Het decentrale server concept is onderdeel van de NII.

Interoperabiliteit en standaardisatie

De gewenste en noodzakelijke interoperabiliteit wordt primair ingegeven door de samenwerkingsverbanden die ontstaan in het kader van de drie hoofdtaken. Defensie moet hierbij een sterke externe focus hebben. Bij het vaststellen van de belangrijkste samenwerkingsverbanden lijkt NAVO voor de komende jaren dominant te zijn maar nemen ook de OOV sector en de EU in belang toe. Daarnaast leert operatie ATALANTA ons dat samenwerken met minder voor de hand liggende partners realiteit is geworden.

Het optreden in diverse samenwerkingsverbanden die ook nog eens frequent wisselen van samenstelling leidt vaak tot situaties dat systemen niet interoperabel zijn. In deze diversiteit en dynamiek bieden het gebruik van Open Standaarden en gestandaardiseerde koppelvlakken oplossingen om informatie alsnog tussen de verschillende partijen te kunnen uitwisselen.

Binnen de extern ingegeven keuzes in het belang van interoperabiliteit moet vanuit het oogpunt van doelmatigheid worden aangestuurd op verregaande interne standaardisatie op systemen, zowel binnen Defensie als binnen de rijksoverheid.

Strategische richtlijnen:

- Defensie maakt primair gebruik van Open Standaarden en als deze er niet zijn die van NAVO.
- Defensie sluit maximaal aan op de NAVO architectuur voor het operationele domein om het hergebruik van software mogelijk te maken.
- Gelet op de dynamiek en de lange termijn werking moet Defensie in het verwervings- en realisatieproces 'onder architectuur' gaan werken en hiervoor een sterkere governance inrichten. Het toezien op en het afdwingen van het gebruik van Open Standaarden is hiervan een integraal onderdeel.
- Interoperabiliteit in het kader van de drie hoofdtaken krijgt bij budgettoewijzing hogere prioriteit dan interne standaardisatie.

Sourcing en partnership

De civiele ontwikkelingen op het gebied van informatietechnologie (IT) gaan vele malen sneller dan ons Defensie Materieelkeuze Proces kan volgen en het innovatief vermogen van de markt is vele malen groter dan dat van Defensie. ICT-infrastructuur wordt op de markt in toenemende mate als dienst (*'Xxx as a Service'*) aangeboden. Veel bedrijven en organisaties die ICT-infrastructuur niet als kerncompetentie beschouwen maken hier al gebruik van, al dan niet via het aangaan van strategische allianties met grote leveranciers. Ook defensieorganisaties van andere landen en grote commerciële partijen zoals SHELL hebben inmiddels aansluiting gezocht met consortia van industriepartners om op grote schaal infrastructuur(services) uit te besteden. Meestal wordt hierbij een uitzondering gemaakt voor de ICT ondersteuning van de kerncompetenties van een bedrijf.
In sourcing vraagstukken en bij het aangaan van strategische partnerships met de industrie is het van belang om vast te stellen in welke mate Defensie zeggenschap moet behouden over infrastructuur ten behoeve van de zogenaamde kerncapaciteiten (EOC'n). Defensie wordt in dit kader onder extreme nationale omstandigheden vaak nog als 'last resort' aangemerkt. Als alle (communicatie) voorzieningen in Nederland uitvallen, moet de Defensie infrastructuur nog blijven werken (vergelijkbaar met het idee van een nationaal noodnet).

Onze defensieorganisatie rekent het HGI, noodvoorzieningen, systemen voor het ontplooide, het mobiele en het uitgestegen domein, ontwikkeling & innovatie en kennisopbouw van missie kritische systemen tot haar kerncapaciteiten. In het kader van snelle ontplooibaarheid en mobiliteit (EOC3) moet Defensie minimaal beschikken over eigen NII capaciteiten voor de 'Initial Entry Forces' met inbegrip van reach-back voor zo klein mogelijke expeditionaire *footprints*. Denk hierbij aan de eerste inrichting voor *deployed* eenheden alvorens de ondersteuning voor de langere termijn in een semi-statische omgeving kan worden overgenomen door *contractors* onder behoud van de kerncapaciteiten. Initiële ontplooiing, mobiel en uitgestegen optreden in het operationele domein vereisen doorgaans specifieke oplossingen voor tijdkritische informatie uitwisseling.

Voorzieningen in de statische infrastructuur, zoals netwerken, reken- en datacentra, kantoorautomatisering en vaste telefonie lenen zich bij uitstek voor grootschalige sourcing bij strategische partners waarbij voortdurende verbetering en efficiency winst moet zijn geborgd. Onder voorwaarden geldt dit ook voor de voorzieningen in een semi-statische omgeving na de initiële ontplooiing bij langdurige inzet.

Strategische richtlijnen:
- Defensie moet optimaal gebruik maken van ICT capaciteiten van derden en houdt daarbij rekening met de eisen op het gebied van beveiliging en continuïteit.
- Defensie moet ICT-infrastructuur maximaal sourcen onder behoud van de noodzakelijke kerncapaciteiten voor de EOC'n.
- Defensie houdt rekening met specifieke eisen voor de initiële ontplooiing en het mobiele en uitgestegen optreden.
- De governance van de totale NII dient altijd in eigen hand te blijven in de rollen van Smart Buyer, Smart Specifier en Smart Integrator (vergelijkbaar met systeemverantwoordelijkheid), inbegrepen regie en vraagarticulatie.

Planning, realisatie en innovatie

Adaptief vermogen (MSV2010) betekent o.a. het snel gebruik kunnen maken van nieuwe middelen en mogelijkheden. Defensie moet zich in deze beraden over wat het kort cyclisch karakter van IT betekent voor het Defensie Materieelkeuze Proces (DMP) en de regelgeving voor aanbestedingen om te voorkomen dat verouderde technologie wordt uitgerold. Enerzijds betekent dit meer aandacht voor het toepassen van 'spiral development' (CD&E) met direct nut voor de operator. Anderzijds moet er meer focus zijn voor de markt en *Commercial off the Shelf* (COTS) met maximale aandacht voor raam- en afroepcontracten. Het uitgangspunt moet zijn dat COTS goed genoeg is, zelfs wanneer COTS niet 100% voldoet aan de eisen. We moeten daarbij duidelijk onderscheid maken tussen eisen en wensen en ook genoegen willen nemen met de 80% oplossing. Dit kan alleen gerealiseerd worden als er sprake is van een continue dialoog tussen gebruiker, behoeftesteller, verwerver en industrie. Het is tevens noodzakelijk om een volledig beeld te hebben van de consequenties van het gebruik van COTS (civiele) technologie in het operationele domein.

Verder moet altijd de afweging tussen het Defensie Investerings Plan (DIP, producten kopen) en het Defensie Exploitatie Plan (DEP, diensten afnemen) worden opgenomen maar dan wel in een bredere context dan nu het geval is bij 1-op-1 vervanging van systemen als gevolg van het einde van de technische of economische levensduur. Het is hierbij van belang om niet alleen te kijken naar (IV en ICT) investeringen maar naar de *Total Cost of Ownership* (TCO) van systemen en diensten in onderlinge samenhang. Het is dan ook van belang om alle bestaande en voorziene capaciteiten binnen de scope van NII samen te brengen onder één portfolio zowel voor wat betreft de exploitatielasten als de begrote investeringen. Besluitvorming moet plaatsvinden op basis van business cases met bijbehorende risicoanalyses binnen de financiële kaders van het totale (NII) portfolio. In een later stadium kunnen de revenuen van genetwerkt samenwerken terugvloeien naar de algemene middelen.

Het wordt steeds belangrijker om onderzoek te focussen op de uitvoering en ondersteuning van onze kerncapaciteiten en het borgen van de specifieke kennis daarvoor. Versterk de dingen die marktpartijen niet doen of waar we als defensieorganisatie niet afhankelijk kunnen en mogen worden van de markt. Om die reden ontwikkelen defensiebedrijven (C2SC, CAMS *Force Vision* en het Research en Innovatie Centrum), in strategisch partnerschap met NAVO (NC3A) en industrie, defensie specifieke oplossingen voor de NII. Het kort cyclisch karakter van IT betekent dat er in de opdracht rekening mee moet worden gehouden dat niet alle eisen en wensen in de initiële behoeftestelling kunnen worden opgenomen. Tevens is het adaptief vermogen van eenheden beperkt, wat betekent dat nieuwe functionaliteit in beperkte ('behapbare') releases moet worden ingevoerd. De operators dienen zoveel mogelijk bij innovatie te worden betrokken door gebruik te maken van oefeningen in de oefenkalender waarin eenheden worden aangewezen voor het testen van stappen in de innovatie (*Proof of Concept*). Omgekeerd kunnen testnetwerken en testomgevingen (C4I en NII in samenhang) een efficiënte bijdrage leveren aan (gevirtualiseerde) oefeningen.

Ten aanzien van interne kennisopbouw en vernieuwing worden C2SC en CAMS *Force Vision* momenteel te zeer belemmerd door de belasting van het beheer van ontwikkelde en geproduceerde systemen. Dit gaat ten koste van innovatiecapaciteit. Door Defensie zelf ontwikkelde systemen leiden doorgaans tot onevenredig grote beheerinspanning door de verschillende versies die ontstaan als gevolg van de korte inzetcycli. Overdracht van het beheer aan reguliere beheerorganisaties en goede samenwerking met de markt is vitaal voor de continuïteit van de bedrijfsvoering.

Strategische richtlijnen:
- Defensie richt zich voor de realisatie van de NII maximaal op de markt (COTS/MOTS) en CD&E.
- Defensie moet investeringen en exploitatie in de ICT-infrastructuur afwegen binnen een integraal NII portfolio en het programmamanagement hiervoor professionaliseren.
- Defensie moet ontwikkelcentra niet belasten met afgeleide taken zoals beheer van ontwikkelde systemen: Defensie ontkoppelt ontwikkeling (innovatiecapaciteit) en beheer.
- Defensie moet innovatief en toekomstgericht zijn en blijven op de ondersteuning van de EOC'n.
- Innovatieactiviteiten worden via CD&E trajecten verbonden aan oefenkalenders voor maximale betrokkenheid van de ontvangende eenheden.
- Nieuwe functionaliteiten moeten onafhankelijk van de inzetcycli in beperkte releases kunnen worden ingevoerd.
- Defensie onderhoudt, in het belang van realisatie en innovatie van de NII, strategische relaties met NAVO (NC3A) en de industrie (o.a. *Network Centric Operations Industry Consortium* (NCOIC) en de Stichting Nederlandse Industrie voor Defensie en Veiligheid of kortweg NIDV).

Personeel, opleiding en training

Werving en behoud van personeel wordt voor een belangrijk deel afhankelijk van wat Defensie kan bieden op het gebied van de moderne, hedendaagse informatietechnologie. De nieuwe generatie defensiemedewerkers verwacht in de NII van Defensie dezelfde mogelijkheden voor o.a. *Unified Communications* en *Social Community Networking* als in de burgermaatschappij. Door deze nieuwe technologie te integreren in de NII neemt de effectiviteit van de medewerkers toe en kan veel efficiënter met (arbeids) tijd en ruimte worden omgegaan.
Defensie vraagt veel verantwoordelijkheden van jonge militairen tijdens uitzendingen,

ook in de kantoorsituatie moet Defensie op die eigen verantwoordelijkheid vertrouwen. De self empowerment van de jeugd biedt kansen, maar kan ook tot risico's leiden, gelet op het gemak waarmee het privéleven wordt prijsgegeven op het internet (Facebook/ Hyves). *Lessons learned* gaan nu vaak over openbaar e-mail! Enerzijds moet Defensie dus meer nog dan in het verleden in opleidingen aandacht besteden aan hoe om te gaan met (defensie) gevoelige informatie in de verschillende media. Anderzijds moet de NII erop ingericht zijn om, transparant voor de operator, gevoelige informatie (waaronder *Lessons Learned*) veilig te versturen vanuit het uitzendgebied naar belanghebbende partijen maar tegelijkertijd ook open communicatie mogelijk te maken met het thuisfront.

Er worden steeds meer externe opleidingen aangeboden over internet waar ook Defensie haar voordeel mee kan doen. Wat extern wordt aangeboden hoeft niet meer zelf te worden ingericht en aangeboden. Door interne opleidingen op afstand over het intranet aan te bieden kan aanzienlijk bespaard worden op het dienstreisbudget.

Het (onderling) koppelen van trainers, simulatoren en eenheden vergroot het effect van opleidingen en training. Meer dan tot nu toe dienen deze koppelingen in de ontwerpfase te worden meegenomen. Door de communicatie tussen trainers en simulatoren over de NII te realiseren is het mogelijk om elke vorm van optreden plaats onafhankelijk joint te simuleren.

Alhoewel door sourcing van ICT diensten vermoedelijk het aantal professionals en specialisten op het gebied van ICT en IV kan worden gereduceerd, blijft er behoefte bestaan aan kennis binnen de eigen organisatie op het gebied van zowel innovatie als beheer.

Strategische richtlijnen:

- Defensie moet in de NII met moderne technologische mogelijkheden de digitale vaardigheden van 'informatiewerkers' benutten.
- Defensie moet bedacht zijn op mogelijke informatiebeveiligingsrisico's die kunnen ontstaan als gevolg van het gebruik van sociale media door de nieuwe generatie medewerkers.
- De NII moet transparant mogelijkheden bieden voor 'gesloten' en 'open' communicatie (vanuit uitzendgebieden).
- De NII moet erop berekend zijn dat opleidingen in principe op afstand via het intranet en/of het internet worden aangeboden.
- Defensie moet het koppelen van trainers, simulatoren en eenheden via, een daarvoor toereikende, NII als uitgangspunt opnemen in het ontwerp en de verwerving van nieuw materieel.
- Defensie borgt aan de EOC'n gerelateerde kennis op het gebied van innovatie en beheer binnen de eigen organisatie.

SAMENVATTENDE CONCLUSIES

- De NII omvat alle middelen om informatie door middel van communicatie en informatie integratie te verwerken, te delen, te presenteren, te beveiligen en het geheel te beheren. Voor de ontwikkeling van de NII staat ondersteuning van het primaire proces (gereedstelling en inzet) centraal.
- De operationele en IV-ambities van Defensie kunnen beter worden gerealiseerd als Defensie - vanuit een gebruikersperspectief - beschikt over één Netwerk en Informatie Infrastructuur waarover beveiligde en onbeveiligde informatie kan worden uitgewisseld met samenwerkende militaire en niet-militaire partners onder alle gebruiksomstandigheden. Tegelijkertijd moeten delen van de Defensie NII geschikt worden gemaakt voor inpassing in de 'NII' van een bepaalde missie of oefening.
- Voor de realisatie van een toereikende, toekomstvaste en betaalbare NII moet in overeenstemming met het belang van informatiedominantie een Defensie brede afweging kunnen plaatsvinden voor de allocatie van middelen. De verwachting is dat hieruit een doelmatigheidswinst te behalen is.

NAWOORD

Voor de HDIO is lkol ir. Jan van de Pol belast met de uitwerking van de strategische visie Netwerk en Informatie Infrastructuur: een Roadmap NII. Vervolgens wordt deze Roadmap NII doorgeleid naar het Joint IV Commando (JIVC) voor verdere uitwerking en betrokken bij het opstellen van de (afgeleide) Projecten Roadmaps en Diensten Roadmaps. Afgeleide Roadmaps die op hun beurt de input vormen voor de JIVC Product *Lifecycle* Plannen.

SCRUBBER DEFENSIE

Kapitein Gert Jan Bergman, Staf CLAS Afdeling IV&CIS Informatiebeveiliging

Data uitwisseling tussen verschillende systemen is anno 2012 gemeengoed geworden. In de militaire werkelijkheid betekent dat bijna onvermijdelijk een tsunami aan NAVO en nationale voorschriften, richtlijnen en aanwijzingen waar aan moet worden voldaan. Immers, data uitwisseling tussen verschillende systemen is niet zonder risico's. Sinds kort kunnen Defensie en de Koninklijke Landmacht over een gecertificeerde scrubber (letterlijk: schoonmaker) beschikken. In dit artikel doet kap Gert Jan Bergman een en ander uit de doeken.

INLEIDING

Betrouwbare data uitwisseling tussen verschillende soorten nationale en internationale netwerken/systemen wordt steeds belangrijker. Deze netwerken/systemen zijn veelal niet gekoppeld. De reden hiervan ligt in het feit dat dit technisch (nog) niet mogelijk en/of niet toegestaan is en/of doordat er een verschil is in rubriceringsniveau en rubriceringsdomein.
Het is niet zondermeer toegestaan om systemen, zonder accreditatie van de Beveiligings Autoriteit (BA), te koppelen met een ongelijk rubriceringniveau of rubriceringsdomein (Bron: DBB UB D/401).

Een voorbeeld hiervan is het koppelen van openbaar 'vuil' internet (Unclassified) aan Titaan 'Rood' (max. Staatsgeheim CONFIDENTIEEL / NATO SECRET): niet toegestaan.
Een tweede voorbeeld. Titaan 'Rood' koppelen aan BICES (NATO SECRET): niet toegestaan.
Het is wel toegestaan om data met een lager rubriceringsniveau te verwerken op een systeem met een gelijk of hoger rubriceringsniveau.

Maar hoe krijg je nu de data op een 'schone' manier van het ene systeem naar het andere door de airgap?

DE VERVUILDE AIRGAP

De data wordt in veel gevallen middels External Storage Devices (ESD) overgezet van het ene naar het andere netwerk/systeem. ESD, veelal USB opslag media, worden steeds meer binnen Defensie gebruikt. Te denken valt aan USB-sticks en USB harde schijven. Daarnaast zijn ook opslagkaartjes

1. Informatie rubricering of merking?
- ONGERUBRICEERD - ONGEMERKT - NATO UNCLASSIFIED
- Dep. VERTROUWELIJK - NATO RESTRICTED - PERSONEELS-VERTROUWELIJK - COMMERCIEEL VERTROUWELIJK - MEDISCH GEHEIM - INTERN BERAAD - INTERN GEBRUIK DEFENSIE
- Stg. CONFIDENTIEEL - NATO CONFIDENTIAL - CONFIDENTIEL UE
- Stg. GEHEIM - NATO SECRET - SECRET UE - ACINT
- Stg. ZEER GEHEIM (buiten scope)

Beknopt overzicht van rubriceringen en merkingen

of storage cards (CF, SD etc.) bij telefoontoestellen en camera's gemeengoed geworden. Maar vergeet ook niet de klassieke cd-rom, dvd en de al bijna 'vergeten' floppy disk.
Het gevaar van deze overdracht is het gebruik van veelal ongecontroleerde ESD met de mogelijkheid tot het verspreiden van kwaadaardige programmatuur. Het afgelopen jaar heeft zich dit meerdere malen voorgedaan waarbij de operationele inzet van het besmette systeem werd belemmerd met alle gevolgen van dien. Het is van belang dat de data en de ESD zelf 'schoon' zijn van kwaadaardige programmatuur en/of software. Bij kwaadaardige programmatuur moet u denken aan virussen, malware, spyware, trojans etc. Schoonmaken: scrubben dus.

DE SCHONE AIRGAP

De Scrubber Defensie of kortweg scrubber biedt de mogelijkheid om de ESD met data te controleren en te schonen van kwaadaardige programmatuur/software. Met de scrubber worden zowel een fysiek doel als een conceptueel/mentaal doel nagestreefd.

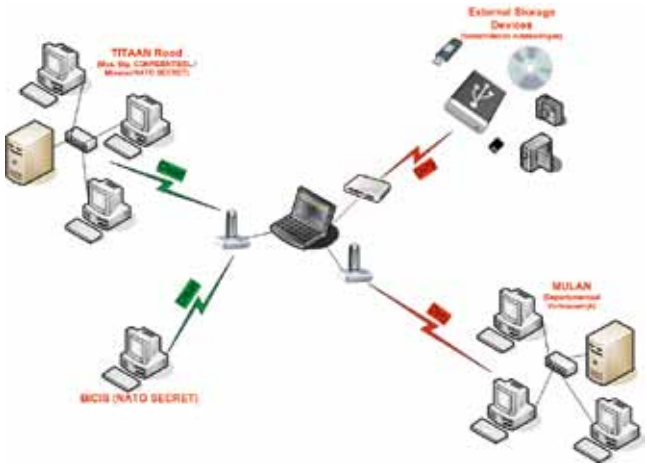
- Ten eerste het fysieke doel: de bescherming van onze eigen netwerken/systemen.
- Ten tweede het conceptuele/mentale doel: vertrouwen wekken bij onze partners dat onze data schoon is.

Wat is de scrubber en hoe gaat de scrubber te werk?

SCRUBBER

Herkenbare scrubber in laptop uitvoering

De scrubber is een standalone laptop die is voorzien van Pointsec Protector (PP) van de firma CheckPoint, bekend van onder andere VSOFT. Daarnaast worden op de scrubber een tweede en een derde antivirusprogramma gebruikt. Uiteraard is het van groot belang dat de laatste updates worden toegepast.
PP is een software pakket dat o.a. waakt over de verschillende poorten (USB, Firewire, Bluetooth etc.) van een computer. Met PP kan men poorten blokkeren/openzetten en bepalen welk type ESD toegang heeft tot een opengestelde poort. Naast deze fysieke instelling controleert PP op toegestane extensies. (bv. doc, docx, txt etc.). Niet toegestane extensies (bv. exe, bat, scr etc.) worden door het systeem geblokkeerd en moeten eerst worden verwijderd voordat de ESD wordt vrijgegeven. Gelijktijdig met de scan op extensies controleert de virusscanner de ESD. Wanneer er een mogelijk virus aangetroffen wordt zal er een akoestisch signaal hoorbaar zijn en wordt de ESD geblokkeerd.
Voldoet de ESD aan alle criteria: juiste poort, toegestane ESD, toegestane extensies en geen virus dan wordt deze vrijgegeven voor gebruik. De vrijgegeven data kan alleen verplaatst worden tussen twee ESD's. Het grote voordeel hiervan is dat er geen data op de harddisk van de laptop terecht komt en hierdoor is het toegestaan om de scrubber voor verschillende rubriceringsniveaus te gebruiken en blijft de scrubber zelf Unclassified. DefCERT heeft een forensisch onderzoek uitgevoerd om te onderzoeken of er sporen van data zijn achter gebleven op de laptop. De uitkomst van dit onderzoek was zeer positief: geen bruikbare data achtergebleven.



Data overslag tussen ongelijkwaardige systemen door tussenkomst van Scrubber

ONTWIKKELING VAN DE SCRUBBER

Het cluster Informatiebeveiliging van Staf CLAS heeft als initiator in de aanloopfase verschillende stakeholders, waaronder: CZSK, CLSK, de BA, DOPS/J6, IVENT en DefCERT (CSM), betrokken bij het opstellen van het pakket van eisen. DefCERT heeft hierbij vooral het technische gedeelte op zich genomen en zij bepalen tevens, vanuit hun expertise, welke extensies toegestaan of geblokkeerd moeten worden. De eerste prototypes van de scrubber zijn door eenheden van het CLAS (KCT, JISTARC) getest tijdens verschillende oefeningen. Met de input van alle stakeholders en de praktijkervaringen die opgedaan zijn tijdens de oefeningen is de scrubber uitgegroeid tot een vertrouwenwekkend product dat de beschikbaarheid van de data verhoogt. Voorwaarde is dat de scrubber juist gebruikt wordt en is voorzien van de laatste virusscanner updates.

OPERATIONELE TOEPASSING

Met ingang van de Police Training Group (rotatie 3) zijn er drie scrubbers ingezet in de Geïntegreerde Politietrainings Missie (GPM). Zowel op de locatie Kunduz als op Mashar e Sharif wordt de scrubber naar tevredenheid ingezet door het C2Ost personeel. Ter ondersteuning van het missiegebied is tevens een scrubber verstrekt aan de Opsroom JCG Stroe die als tweedelijns ondersteuning optreedt voor het C2Ost personeel in het missiegebied. Naast technische ondersteuning zorgt de Opsroom ook voor de verspreiding van de essentiële virusscanner updates. De escalatieniveaus voor de Opsroom JCG Stroe zijn, voorlopig, het cluster Informatiebeveiliging van Staf CLAS en DefCERT.

VERDERE TOEPASSING BINNEN CLAS

Momenteel is het proces gestart om de Scrubber Defensie als IT-dienst of product te laten ontwikkelen en op te nemen in de dienstencatalogus van IVENT. Op korte termijn verwacht IVENT aan de operationele behoefte te kunnen voldoen door 50 laptops beschikbaar te houden. Deze 50 scrubbers worden in overleg met de Beveiligings Coördinator CDS (BC-CDS) en op aangeven van het cluster Informatiebeveiliging van Staf CLAS naar de CLAS eenheden geleid.