Ministerie van Defensie

NEDERLAND ICT

ICT Haalbaarheidstoets

Doorontwikkeling IT

12 & 26 juni 2015

Rapportage

Definitief

Versie 1.0

Datum 20 juli 2015

Inhoudsopgave

Managementsamenvatting Eerste Workshop

Is het voorgestelde samenwerkingsmodel werkbaar en toekomstvast?

De marktpartijen zijn van mening dat het voorgestelde samenwerkingsmodel werkbaar kán zijn. Ze missen echter nog veel details in de uitwerking. In het bijzonder de regie- en integratiefunctie van Defensie ten opzichte van de rol en verantwoordelijkheden van marktpartijen is aanleiding voor opmerkingen. De nadere uitwerking kan al onderdeel zijn van de beoogde samenwerking. Zo geven de marktpartijen aan dat Defensie de regie en integratie niet volledig zelf hoeft te doen, maar marktpartijen, al dan niet als samenwerkingsverband, kan selecteren om een afgebakend deel van doorontwikkeling IT voor hun rekening te nemen. Het is dus voor Defensie van belang naast de indeling van het IT domein ten behoeve van de verwerving een onderscheid te maken in de rol die marktpartijen voor hen kunnen spelen. De voorgestelde indeling van het IT domein ten behoeve van de verwerving sluit niet meer goed aan bij de wijze waarop marktpartijen nu al vaak producten en diensten aanbieden. O.a. door ontwikkelingen van clouddiensten en beveiligingsdiensten zijn er ook andere mogelijkheden. De indeling in hoog of laag gerubriceerde informatie of statisch en ontplooide IT is dan niet in alle situaties zo toepasbaar.

Kan Defensie haar regierol dragen en de expertise van marktpartijen benutten?

Defensie kan de regie- en integratierol vervullen als het haar lukt marktpartijen in hun kracht te benutten. Dat vraagt dat regie vanuit overzicht en samenhang wordt gedaan, als verbinding tussen de business (proceseigenaren) van Defensie en de mogelijkheden van de marktpartijen. Het gaat dan niet alleen om de IT componenten, maar ook om de verandering die Defensie met behulp van IT wil maken. Regie en integratie is dan een verantwoordelijkheid van Defensie én marktpartijen, die op basis van een goede taakverdeling en met kleine stapjes wordt gerealiseerd. De regie is het organiseren van de vraag en het aanbod. Enterprise architectuur, portfoliomanagement helpt daarbij, maar requirements management en verandermanagement ook. Het onderscheid tussen continuïteit en innovatie is niet altijd goed te maken, want soms is innovatie een integraal onderdeel van de af te nemen dienst of het voortdurende verandertraject. De detachering van personeel over en weer is een goede manier om kennis en ervaring uit te wisselen en beter samen op te trekken in de doorontwikkeling. Houd hierbij de hiërarchie helder: er kan maar één baas zijn.

Kunnen Defensie en markt tot passende afspraken komen?

De marktpartijen raden aan de selectie van leveranciers en de inhoud en het managen van contracten goed aan te laten sluiten op de eisen vanuit regie. De aard en duur van de relatie met de leveranciers, het betrokken deel van het IT domein ten behoeve van de verwerving, de al dan niet daarin opgenomen vernieuwing en de in te zetten expertise bepalen de contractuele voorwaarden en prijsmodellen. Het samenwerkingsmodel stelt hoge eisen aan procurement. De marktpartijen raden dan ook aan daarin blijvend te

investeren en meer gebruik te maken van de mogelijkheden die de aanbestedingswetten bieden om ook op inhoudelijke criteria te selecteren.

Managementsamenvatting Tweede Workshop

Is het voorgestelde samenwerkingsmodel werkbaar en toekomstvast?

De marktpartijen verwachten dat het samenwerkingsmodel goed kan werken en toekomstvast is. Ze zien als risico dat er een te grote verscheidenheid aan leveranciers met verschillende contractuele voorwaarden ontstaat, die alle door Defensie minutieus moeten worden aangestuurd. Bovendien is het risico dat de indeling van het IT domein ten behoeve van de verwerving niet past bij hoe marktpartijen, al dan niet in onderlinge samenwerking, best practices in IT- of Defensie-ketens kunnen toepassen of dat de overgang van bestaande naar nieuwe IT minder snel gaat dan wellicht mogelijk is. De marktpartijen stellen voor dat Defensie steeds op voorhand informatief overleg voert met relevante marktpartijen om functioneel uit te kunnen vragen en de samenwerking goed te richten op wat Defensie wil bereiken. Het definiëren van behapbare brokken inclusief de gevraagde continuïteit en innovatie krijgt dan vorm via co-creatie in plaats van micromanagement. Defensie heeft zelf de regie, vooral wat betreft uitwerking van de strategie in architectuur en aanpak, gebaseerd op haar organisatie en kennis van de vraag.

Kan Defensie haar regierol dragen en de expertise van marktpartijen benutten?

De marktpartijen zijn van mening dat het noodzakelijk is dat Defensie zelf de regie voert. Zij kan zich daarbij door de marktpartijen en door de regiepartner laten ondersteunen. Maar ook bij de uitwerking van het High Level Ontwerp, in de architectuurfuncties en in het programmamanagement heeft Defensie zelf de eindregie op het organiseren van vraag en aanbod. Ze kan door middel van verschillende vormen van leveranciersoverleg een verwervingsvraag goed voorbereiden, een deel van het IT domein ten behoeve van de verwerving afbakenen en in beheersbare stappen laten uitvoeren. Zo kan Defensie de best practices van marktpartijen en andere opdrachtgevers optimaal benutten. Om dat te kunnen doen raden de marktpartijen Defensie aan te investeren in het eigen personeel, zowel ten behoeve van de regie als ten behoeve van continuïteit en innovatie. Inzet van personeel van Defensie bij marktpartijen is daarnaast goed mogelijk, zeker wanneer hun kennis actueel is en blijft.

Kunnen Defensie en markt tot passende afspraken komen?

De marktpartijen zien op basis van hun ervaring met andere opdrachtgevers voldoende mogelijkheden om tot passende prijsafspraken en contracten te komen. Het vraagt wel een andere opstelling en kennis en expertise van Defensie zelf. In het bijzonder is het op basis van passend vooroverleg komen tot een goede verwervingsvraag, selectiecriteria, service levels én selectiemethode van belang. Dan kunnen marktpartijen al dan niet als samenwerkingsverband ingaan op de verschillende aspecten als inzet van personeel van Defensie, prijsmodel, resultaatgerichtheid en het leveren van continuïteit én innovatie. De aanbestedingsprocedure moet echter wel worden aangepast, sneller en flexibeler,

waardoor beter kan worden meebewogen met de snelle ontwikkeling van markt en technologie.

1 Inleiding

1.1 Aanleiding

De IT van Defensie gaat ingrijpend op de schop. Dat was de conclusie na diverse onderzoeken in 2014 over de staat van IT bij het ministerie. Het ministerie van Defensie heeft hiertoe een visie ontwikkeld 'let's make IT happen!'. De aanpassingen aan de huidige IT worden de komende jaren stapsgewijs ingevoerd. De CIO heeft een High Level Ontwerp document opgesteld dat richting geeft aan deze ontwikkeling. Daarbij maakt Defensie een aantal keuzen ten aanzien van de gewenste samenwerking met de markt. Het ministerie van Defensie, in het bijzonder de programmaorganisatie Vernieuwing, wil de haalbaarheid op een aantal aspecten laten toetsen middels een ICT Haalbaarheidstoets, voordat zij een eerste aanbesteding binnen deze vernieuwde kaders doet.

1.2 ICT Haalbaarheidstoets

De ICT Haalbaarheidstoets is een instrument van brancheverenigingen Nederland ICT dat door de Rijksoverheid ingezet wordt om in een vroegtijdig stadium in de markt pre-competitief te toetsen of een strategie voor een project of aanbesteding haalbaar en realistisch is. De toets is ontwikkeld in samenwerking met de ministeries van BZK en EZ, is onderdeel van de iDialoog (de samenwerking tussen Rijk en ICT-bedrijfsleven) en wordt sterk gestimuleerd vanuit de Rijksoverheid.

De ICT Haalbaarheidstoets wordt onder verantwoordelijkheid van de projectleider van Nederland ICT uitgevoerd. Uitvoering geschiedt voor een groot deel door PBLQ HEC. Dit is de 27ste ICT Haalbaarheidstoets.

Het proces om de ICT Haalbaarheidstoets uit te voeren bestaat uit zes opeenvolgende stappen:

- *Stap 1: De vraagstelling*
  Een Rijksoverheidsorganisatie komt met een vraag, concept of idee naar Nederland ICT om voor te leggen aan ICT-bedrijven. Nederland ICT formuleert in overleg een heldere vraagstelling en doet een aankondiging van de ICT Haalbaarheidstoets aan de markt.

- *Stap 2: Deelnemers workshop*
  In overleg met Nederland ICT selecteert de vragende Rijksoverheidsorganisatie een aantal ICT-bedrijven dat wil deelnemen aan de workshop.

- *Stap 3: De workshop*
  Nederland ICT organiseert een workshop waarin de deelnemers discussiëren over de haalbaarheid van de vraag, het concept of idee. Ook de vragende Rijksoverheids-organisatie neemt actief deel aan de workshop.

- *Stap 4: De conceptrapportage*
  Op basis van de resultaten van de workshop stelt Nederland ICT een concept-rapportage op.

- *Stap 5: De tweede ronde*
  Nederland ICT legt de conceptrapportage voor aan de deelnemers van de workshop. Op individuele basis kunnen zij schriftelijk reageren en aanvullingen geven.

- *Stap 6: De definitieve toets*
  Waar mogelijk verwerkt Nederland ICT de aanvullingen van de workshopdeelnemers. Nederland ICT biedt de eindrapportage over de ICT Haalbaarheidstoets aan de vragende Rijksoverheidsorganisatie aan.

1.3 Aanpak

Conform het concept van de ICT Haalbaarheidstoets zijn de volgende stappen uitgevoerd:
- De uitnodiging van Defensie, NIDV en Nederland ICT voor deelname aan de ICT Haalbaarheidstoets is op 28 mei 2015 gepubliceerd. De uitnodiging bevat de vragen van Defensie aan de markt;
- Een deel van de partijen die zich hebben aangemeld zijn uitgenodigd voor deelname aan de workshop op 12 juni 2015. Op 26 juni 2015 is met de resterende partijen een tweede uitvoering van de ICT Haalbaarheidstoets gehouden. De lijst met deelnemers van beide workshops is opgenomen in bijlage A;
- In de workshop zijn de deelnemende bedrijven (de markt) en Defensie onder begeleiding van PBLQ HEC aan drie tafels in drie ronden en een gezamenlijke slotronde interactief in gesprek gegaan over de vragen van Defensie;
- Onder auspiciën van Nederland ICT is het resultaat van de workshop verwerkt in een geanonimiseerde conceptrapportage;
- De conceptrapportage is per workshop aan de markt voorgelegd voor commentaar. Daarna zijn de rapportages van de workshops samengevoegd en is het rapport definitief gemaakt en namens de markt aangeboden aan Defensie;
- Het eindrapport is openbaar gemaakt via de website van Nederland ICT, en is tevens aan de deelnemende bedrijven toegestuurd.

1.4 Indeling rapport

De indeling van het rapport is als volgt:

1. Hoofdstuk 2 beschrijft de vragen van Defensie aan de markt over haar samenwerkings-model met de markt bij de doorontwikkeling van haar IT. Het betreft drie hoofdvragen over de haalbaarheid, regie en contractuele modellering.
2. Deze drie hoofdvragen komen aan de orde in de hoofdstukken 3, 4 en 5. Elk hoofdstuk begint in de eerste paragraaf met herhaling van de vraag van Defensie.

Daarna volgt een samenvatting van het antwoord van de markt op de vraag[1]. De derde paragraaf beschrijft de diverse (aandachts)punten die de marktpartijen aan Defensie ter overweging geven. *De verschillende inbreng van de markt tijdens de twee workshops is als aparte managementsamenvatting en in delen van de hoofdstukken 3-5 opgenomen.*

3. In hoofdstuk 6 vatten de marktpartijen en Defensie hun conclusies van de toets samen in de vorm van een aantal opmerkingen.
4. Bijlage A bevat de lijst van deelnemers aan de workshop.
5. Bijlage B geeft de toelichting en achtergrondinformatie over doorontwikkeling IT en het voorgenomen samenwerkingsmodel, zoals de aan de workshop deelnemende partijen ook hebben ontvangen.

Voor meer informatie of vragen inzake dit rapport kunt u contact opnemen met Nederland ICT: Floor Lekkerkerker of Liesbeth Holterman, tel. 0348 – 49 36 36 of via e-mail: haalbaarheidstoets@nederlandict.nl.

[1]Dit rapport hanteert vaak het begrip 'de markt', hoewel niet in alle gevallen alle deelnemers een bepaalde mening onderschrijven. Dit rapport geeft het gemeenschappelijke beeld van de (meerderheid van de) aanwezige partijen.

2 Vraagstelling

Het ministerie van Defensie wil, aansluitend op de door Defensie ontwikkelde visie 'let's make IT happen!', de verdere ontwikkeling van haar IT in samenwerking met de markt realiseren en beheren. De CIO heeft daartoe een High Level Ontwerp document opgesteld dat richting geeft aan de blijvende ontwikkeling. Daarbij maakt Defensie een aantal keuzen ten aanzien van de gewenste samenwerking met de markt. Een en ander is beschreven in het bijgevoegde document "Samenvatting High Level Ontwerp" (bijlage B). Defensie wil de strategische keuzen middels een drietal hoofdvragen op het gebied van het samenwerkingsmodel, de regierol en afspraken/contracten graag toetsen op haalbaarheid bij de markt voordat zij een eerste aanbesteding binnen deze vernieuwde kaders doet.

Vragen aan de markt

Het ministerie van Defensie wil in de ICT Haalbaarheidstoets de volgende vragen stellen:

1. Is het voorgestelde samenwerkingsmodel werkbaar en toekomstvast? Welke risico's ziet de markt en welke verbetering van het model is mogelijk?

Uitgaande van de beschreven karakteristieken:

- De samenwerking betreft nieuwe IT en verschilt voor hoog en laag gerubriceerde informatie enerzijds en statische en ontplooide IT anderzijds (zie figuur 1);
- De samenwerking betreft meerdere partijen na selectie op verschillende momenten voor afgebakende onderdelen (zie figuur 6);
- Defensie houdt zelf de regie- en integratiefunctie (zie figuren 2 en 3).

2. Kan Defensie in dit samenwerkingsmodel haar regierol dragen en de expertise van de marktpartijen optimaal benutten? Welke risico's ziet de markt en welke versterking van de rol van Defensie en marktpartijen is mogelijk?

Met de genoemde uitgangspunten:

- Er worden meerdere leveranciers ingezet voor de verschillende onderdelen;
- Personeel van Defensie zal zowel onder aansturing van Defensie zelf als van marktpartijen een rol in het beheer vervullen;
- Incrementele aanpak in de doorontwikkeling;
- Onderscheid tussen continuïteit en innovatie in de opdrachtverstrekking;
- Inzet op Enterprise Architectuur en Project Portfolio Management als instrumenten voor de gewenste integraliteit en goed opdrachtgeverschap.

3. Kan Defensie tot voor Defensie en marktpartijen passende prijsafspraken en contracten komen?

Waarbij Defensie streeft naar:

- Selectie van marktpartijen voor afgebakende onderdelen op basis van prijs/ prestatie, "cultural fit" en perspectief voor medewerkers;
- De afgebakende onderdelen zijn voldoende groot en marktconform en kennen een gefaseerd migratiepad;
- De samenwerkingsovereenkomst(en) kennen voldoende flexibiliteit t.b.v. toekomstige uitbreiding en/of innovatie;
- Een externe partij investeert in de nieuwe IT-infrastructuur en neemt dat op in de tarieven voor dienstverlening;
- Defensie onderscheidt continuïteit en innovatie in de contracten en budgetten;
- Defensie houdt zelf de overall regie, maar kan afgebakende onderdelen van Ontwikkelen en Beheren als resultaatopdracht aan marktpartijen gunnen.

3 Is het samenwerkingsmodel werkbaar en toekomstvast?

3.1 De vraag van Defensie

Is het voorgestelde samenwerkingsmodel werkbaar en toekomstvast? Welke risico's ziet de markt en welke verbetering van het model is mogelijk?

Uitgaande van de beschreven karakteristieken:

- De samenwerking betreft nieuwe IT en verschilt voor hoog en laag gerubriceerde informatie enerzijds en statische en ontplooide IT anderzijds (zie figuur 1);
- De samenwerking betreft meerdere partijen na selectie op verschillende momenten voor afgebakende onderdelen (zie figuur 6);
- Defensie houdt zelf de regie- en integratiefunctie (zie figuren 2 en 3).

De marktpartijen hebben deze vraag in drie groepen in aanwezigheid van vertegenwoordigers van Defensie besproken. Paragraaf 3.2 geeft een samenvatting van de bespreking. Paragraaf 3.3 geeft de aandachtspunten en opmerkingen van de marktpartijen in de vorm van korte alinea's weer.

3.2 Het samenvattende antwoord van de markt

Eerste Workshop

De marktpartijen zijn van mening dat het voorgestelde samenwerkingsmodel werkbaar kán zijn. Ze missen echter nog veel details in de uitwerking. In het bijzonder de regie- en integratiefunctie van Defensie ten opzichte van de rol en verantwoordelijkheden van marktpartijen is aanleiding voor opmerkingen. De beoogde uitwerking kan al onderdeel zijn van de beoogde samenwerking. Zo geven de marktpartijen aan dat Defensie de regie en integratie niet volledig zelf hoeft te doen, maar marktpartijen, al dan niet als samen-werkingsverband, kan selecteren om een afgebakend onderdeel van doorontwikkeling IT voor hun rekening te nemen. Het is dus voor Defensie van belang naast de indeling van het IT domein ten behoeve van de verwerving een onderscheid te maken in de rol die marktpartijen voor hen kunnen spelen. De voorgestelde indeling van het IT domein ten behoeve van de verwerving sluit niet meer goed aan bij de wijze waarop marktpartijen nu al vaak producten en diensten aanbieden. O.a. door ontwikkelingen van clouddiensten en beveiligingsdiensten zijn er ook andere mogelijkheden. De indeling in hoog of laag gerubriceerde informatie of statisch en ontplooide IT is dan niet in alle situaties zo toepasbaar.

Tweede Workshop

De marktpartijen verwachten dat het samenwerkingsmodel goed kan werken en toekomstvast is. Ze zien als risico dat er een te grote verscheidenheid aan leveranciers

met verschillende contractuele voorwaarden ontstaat, die alle door Defensie minutieus moeten worden aangestuurd. Bovendien is het risico dat de indeling van het IT-domein ten behoeve van de verwerving niet past bij hoe marktpartijen, al dan niet in onderlinge samenwerking, best practices in IT- of Defensie-ketens kunnen toepassen of dat de overgang van bestaande naar nieuwe IT minder snel gaat dan wellicht mogelijk is. De marktpartijen stellen voor dat Defensie steeds op voorhand informatief overleg voert met relevante marktpartijen om functioneel uit te kunnen vragen en de samenwerking goed te richten op wat Defensie wil bereiken. Het definiëren van behapbare brokken inclusief de gevraagde continuïteit en innovatie krijgt dan vorm via co-creatie. Defensie heeft zelf de regie, vooral wat betreft uitwerking van de strategie in architectuur en aanpak, gebaseerd op haar organisatie en kennis van de vraag. Defensie moet niet in de val trappen om naast regievoering ook aan micromanagement te doen: de marktpartijen kunnen dan ook hun rol optimaal vervullen.

3.3 Aandachtspunten en opmerkingen van marktpartijen

3.3.1 Eerste Workshop

De samenwerking betreft nieuwe IT en verschilt voor de onderscheiden niveaus

Aan de verschillende tafels merken de marktpartijen op dat ze enerzijds deze indeling kunnen en zullen volgen en anderzijds een andere indeling en verdeling misschien voor Defensie tot een betere samenwerking kan leiden. De indeling in hoog en laag gerubriceerde informatie valt *voor een deel* samen met voor Defensie specifieke en generieke, breder inzetbare IT. Evenzo is statisch en ontplooid (in missies) een herkenbaar onderscheid voor inzet van middelen en personeel uit de markt. De marktpartijen wijzen erop dat zowel hedendaagse en toekomstige technologieën, als de diensten van markt-partijen, zich veelal niet volgens deze criteria indelen, ook niet wat betreft bestaande en nieuwe IT. Marktpartijen geven aan dat het steeds gebruikelijker is IT in de vorm van diensten aan te bieden. Via de diensten zijn dan verschillende componenten geïntegreerd of is bijvoorbeeld data beveiligd. Een aantal marktpartijen stelt voor om andere combinaties van diensten, applicaties en/of infrastructuurproducten (stacks) te maken en zo integratie voor en door Defensie te vereenvoudigen. Andere indelingen zijn bijvoorbeeld horizontaal (infrastructuur, cloud, toepassingen) of functioneel (werkplek, ERP, HGI, LGI, ontplooid, statisch).

Het samenwerkingsmodel

De marktpartijen geven aan dat de samenwerking verschillende dimensies heeft. Het gaat niet alleen om de samenwerking tussen Defensie en één of meerdere marktpartijen, maar ook om de samenwerking tussen de marktpartijen onderling. Een bijzonder aandachtspunt daarbij is de dynamiek zowel bij Defensie als in de markt. Defensie heeft te maken met de binnenlandse en internationale ontwikkelingen. De markt zelf ontwikkelt zich ook met nieuwe aanbieders en consolidaties.

In het huidige voorstel is de ruimte voor handelen en/of verantwoordelijkheid dragen door marktpartijen niet heel erg duidelijk. De marktpartijen stellen voor een onderscheid te maken in verschillende typen marktpartijen, b.v. in de mate van het kunnen dragen van risico of de rol die ze voor Defensie kunnen spelen op een kleiner of groter domein. Per type marktpartij kan dan een ander selectietraject worden ingericht en criteria voor goed presteren worden afgesproken. Het is daarvoor van belang dat zowel Defensie als de marktpartijen zo transparant mogelijk zijn over wat hen beweegt; welke belangen en criteria voor hen het belangrijkst zijn. De nagestreefde samenwerking met Defensie en tussen de marktpartijen onderling dient volgens de marktpartijen niet vrijblijvend te zijn, maar een onderdeel van de te controleren afspraken. Daarbij kan Defensie het aantal partijen in eerste instantie ook beperken, om zelf goed regie te kunnen houden.

Het verhelderen van de verwachtingen over en weer is ook van belang voor de keuze die partijen maken voor het al dan niet, of gezamenlijk inschrijven in selectietrajecten door Defensie. Bijvoorbeeld of het gaat om inspannings- of resultaatopdrachten of om een deel- of ketenverantwoordelijkheid.

Omdat een gedetailleerde uitwerking van het samenwerkingsmodel mogelijk zeer lang zou duren om volledig uit te werken in delen van het IT domein ten behoeve van de verwerving en selectieleidraden, raadt de markt Defensie aan dit samenwerkingsmodel en de uitwerking ervan als een reis te zien, waarin in kleinere, beheersbare stappen samen met de markt geleerd wordt. Bij het inrichten van de reis kunnen modellen als het 9-vlaksmodel behulpzaam zijn.

Meerdere partijen op verschillende momenten voor afgebakende onderdelen

Defensie stelt voor om voor afgebakende onderdelen van het IT domein ten behoeve van de verwerving, op verschillende momenten leveranciers te selecteren, en daarbij een onderscheid te maken tussen huidige en nieuwe IT, plus innovatie en continuïteit. De marktpartijen geven aan dat er veel raakvlakken zijn tussen de geschetste indeling van het IT domein ten behoeve van de verwerving, en dat deze nu nog niet erg scherp gedefinieerd zijn. Met name voor de kritische processen van Defensie is dat van belang. Marktpartijen erkennen dat een indeling van het IT domein ten behoeve van de verwerving nodig is, maar stellen wel dat deze voorgestelde indeling niet goed aansluit bij de nieuwe technologische mogelijkheden of de wijze waarop veel marktpartijen diensten aanbieden. Het IT domein ten behoeve van de verwerving kan ook anders worden ingedeeld, bijvoorbeeld naar soorten diensten (beveiligings-, cloud-, applicatiediensten). Een bijzonder aandachtspunt bij de indeling en de selectie van leveranciers is het lifecycle management van de IT componenten. In een aantal van de mogelijk af te nemen diensten is innovatie en continuïteit integraal onderdeel van de dienst (zowel in ter beschikking stellen van computercapaciteit (cloud) als van applicaties (pakketten). De markt vindt dat de potentiële wisseling van dienstverleners op lopende diensten, vanuit het oogpunt van continuïteit en ermee vervlochten innovatie, vooral die innovatie niet optimaal zal bevorderen.

Om de uitwisselbaarheid van producten, diensten en leveranciers in de toekomst mogelijk te maken is het gebruiken van open standaarden en koppelvlakken, zoals bijvoorbeeld bij

cloud standaarden (NIST), van belang. Deze zijn zelf ook in ontwikkeling, dus het is van belang dat Defensie daar goed toegang toe heeft; zelf of via de leveranciers.

Defensie houdt zelf de regie- en integratiefunctie

De marktpartijen hebben nog veel vragen en opmerkingen bij de regie- en integratiefunctie. Zo is binnen Defensie de rol van de CDS en de eigen besturing niet duidelijk. Voor de marktpartijen zelf is de vraag hoe de verschillende denkbare vormen van regie in dit model een plaats hebben, zoals bijvoorbeeld: strategische, tactische of operationele regie, regie op de keten, regie op generieke IT of specifieke IT, regie op verwachtingen. Zij zien de goede invulling van de regierol als essentieel voor de transformatie die Defensie met behulp van IT gaat maken.

Marktpartijen vragen zich af hoe zij individueel of als samenwerkingsverband in de regie een rol kunnen spelen. Zij stellen dat Defensie niet alle regie zelf hoeft te voeren, maar delen daarvan kan overdragen aan (een combinatie van) marktpartijen. Dit in relatie tot de eerdergenoemde andere combinaties van producten of diensten (stacks). Eén of meerdere marktpartijen kan zelf verantwoordelijkheid dragen voor een deel van de doorontwikkeling IT. Het is dan wel van belang om, dat wat Defensie wil en verwacht, goed te definiëren en op de uitvoering ervan toe te zien; een uitwerking van requirements management, maar ook van wat goede regie is. De verbinding tussen wat de eindgebruikers (business) van Defensie nodig hebben en wat de IT-leveranciers kunnen leveren, kan via de regie- en integratierol gerealiseerd worden.

3.3.2 Tweede Workshop

De samenwerking betreft nieuwe IT en verschilt voor de onderscheiden niveaus

De marktpartijen geven aan dat zowel de beperking tot nieuwe IT voor het samenwerkingsmodel, als de onderscheiden niveaus niet ingaan op de overgang van bestaande naar nieuwe IT, noch op de samenwerking in een IT- of Defensieketen. Marktpartijen kunnen bij de overgang van bestaand naar nieuw een positieve rol spelen als er zodanige afspraken gemaakt kunnen worden dat dat voor zowel een latende als ontvangende partij de moeite waard is. Een samenwerkingsmodel, dat aansluit bij de inrichting van de samenwerking ten behoeve van het functioneren van een IT keten (stapeling van IT diensten en producten tot een werkend IT geheel) of Defensie keten (bundeling van diensten producten tot een voor een Defensie domein werkend geheel).

Het onderscheid tussen hoog en laag gerubriceerde informatie is voor veel marktpartijen herkenbaar. Maar tegelijkertijd geven ze aan dat beveiliging in vrijwel alle producten en diensten is verwerkt en op verschillende manieren kan worden ingericht. Zo zijn werkplek en data andere mogelijke aangrijpingspunten voor de beveiliging van informatie.

Om binnen het samenwerkingsmodel voldoende innovatie te houden, verwijzen de marktpartijen naar positieve ervaringen met de inrichting van een aparte innovatie-organisatie bij andere organisaties, zoals de Belastingdienst. Bijvoorbeeld een Broedkamer of

Innovatieloket waar Defensie en marktpartijen, los van lopende opdrachten, samenwerken. Het gaat hierbij voor zowel Defensie als bedrijven om een innovatie op de dienst of product zelf én om de wijze van aanbieden.

Het samenwerkingsmodel

De marktpartijen constateren dat het samenwerkingsmodel ook voor hen kan werken. Ze vragen aandacht voor de uitwerking van de visie samen met de marktpartijen naar architectuur en beveiligings- (cyber) oplossingsrichtingen. Aandachtspunten daarbij zijn de overdraagbaarheid van producten en diensten tussen leveranciers en het als Defensie kunnen blijven innoveren terwijl de continuïteit geborgd is.

De marktpartijen vinden het van belang dat Defensie een vorm van co-sourcing inricht, zodat Defensie en marktpartijen gezamenlijk de incrementele aanpak, maar ook lifecycle management, kunnen vormgeven. Marktpartijen onderschrijven de wens van Defensie om in kleine stappen te werken en op basis van behapbare brokken steeds de werking van de doorontwikkeling van IT aan te tonen. Daarbij kunnen de mensen van Defensie en die van de marktpartijen zich evolutionair ontwikkelen in de samenwerking.

Meerdere partijen op verschillende momenten voor afgebakende onderdelen

De marktpartijen wijzen erop dat dit uitgangspunt ertoe kan leiden dat er een grote verscheidenheid aan partijen kan ontstaan die alle een verschillende contractuele relatie met Defensie hebben. Door functioneel uit te vragen, al niet dan niet in relatie tot een keten, kun je als Defensie meer gebruik maken van de kracht van marktpartijen. Dit in tegenstelling tot de ervaring bij (te) gespecificeerd uitvragen. De marktpartijen stellen voor dat Defensie ter voorbereiding op een uitvraag in overleg gaat met voor die vraag relevante partijen, b.v. in de vorm van een community board. In zo'n board kan Defensie dan zowel gevestigde bedrijven als start-ups betrekken. Het maakt het voor Defensie mogelijk informatie te verzamelen om de wederzijds best passende vraag te stellen. De markt kan zich daarop organiseren, en ook de aanbestedingsregels bieden daarvoor voldoende ruimte.

De afbakening van een deel van het IT domein ten behoeve van de verwerving kan daarbij steeds afgewogen worden. De marktpartijen wijzen op het onderscheid tussen kritische en niet-kritische IT-landschappen en de relatie met het voeren van regie op de IT-ketens en over de delen van het IT domein ten behoeve van de verwerving heen. Maar ook op het kunnen vormen van samenwerkingsverbanden door marktpartijen om aan de gestelde vraag te voldoen. Door de samenwerkingsverbanden kan het voor Defensie eenvoudiger zijn om eindregie te hebben en contracten te sluiten met een beperkter aantal partijen, en tegelijkertijd voldoende ruimte te houden om ook nieuwe partijen toe te laten.

Door de combinatie van marktpartijen voor de bestaande IT en voor de doorontwikkeling van de IT, plus de voortdurende wijziging ten gevolge van aflopende of nieuwe contracten kunnen gemakkelijk fricties over aansprakelijkheid ontstaan. Het is zaak deze frictie tussen marktpartijen, die op basis van verschillende contracten en/of mantelovereenkomsten voor

hardware, software of diensten werken, te voorkomen. Een mogelijkheid ligt in het inrichten van passende prijsafspraken en een geleidelijke overgang. Banken en verzekeraars kunnen daarin een voorbeeld zijn voor Defensie.

Defensie houdt zelf de regie- en integratiefunctie

De marktpartijen onderschrijven dat Defensie zelf de regie heeft en dat de beschreven regiepartner in de eerste plaats een kennispartner is die Defensie ondersteunt bij de interne en externe regie. Goede regie voeren vraagt wel wat van Defensie als werkgever om de daarvoor geschikte mensen (blijvend) te kunnen inzetten. Ook is het ontwikkelen en onderhouden van de noodzakelijke IT-kennis van belang. Dat kan bijvoorbeeld in de vorm van een competence center, waaraan de markt een bijdrage kan leveren.

Bij het voeren van regie kan Defensie gebruik maken van waar de markt goed in is. Dat kan ook regie op technische uitvoering zijn of integratie van best of breed oplossingen. Defensie kan er daarbij voor zorgen dat elke betrokken marktpartij een passende rol vervult, om maximaal gebruik te maken van best practices voor de in te zetten diensten of producten.

De marktpartijen hebben positieve ervaring met het in gezamenlijke teams inzetten van personeel van Defensie en marktpartijen. De betrokkenheid bij het team en het te behalen resultaat is groot. Wel wijzen de marktpartijen op een aantal randvoorwaarden, zoals een goede intake op basis van wederzijds gewenste kwaliteit (actuele kennis), transparantie over toekomstige reorganisaties en eventuele boventalligheid en helderheid over prioriteiten voor de betrokken medewerkers.

4 Kan Defensie haar regierol dragen én de expertise van de markt benutten?

4.1 De vraag van Defensie

Kan Defensie in dit samenwerkingsmodel haar regierol dragen en de expertise van de marktpartijen optimaal benutten? Welke risico's ziet de markt en welke versterking van de rol van Defensie en marktpartijen is mogelijk?

Met de genoemde uitgangspunten:

- Er worden meerdere leveranciers ingezet voor de verschillende onderdelen;
- Personeel van Defensie zal zowel onder aansturing van Defensie zelf als van marktpartijen een rol in het beheer vervullen;
- Incrementele aanpak in de doorontwikkeling;
- Onderscheid tussen continuïteit en innovatie in de opdrachtverstrekking;
- Inzet op Enterprise Architectuur en Project Portfolio Management als instrumenten voor de gewenste integraliteit en goed opdrachtgeverschap.

De marktpartijen hebben deze vraag in drie groepen in aanwezigheid van vertegenwoordigers van Defensie besproken. Paragraaf 4.2 geeft een samenvatting van de bespreking. Paragraaf 4.3 geeft de aandachtspunten en opmerkingen van de marktpartijen in de vorm van korte alinea's weer.

4.2 Het samenvattende antwoord van de markt

Eerste Workshop

Defensie kan de regie- en integratierol vervullen als het haar lukt marktpartijen in hun kracht te benutten. Dat vraagt zowel dat regie vanuit overzicht en samenhang wordt gedaan, als dat de verbinding tussen de business (proceseigenaren) van Defensie en de mogelijkheden van de marktpartijen wordt georganiseerd. Het gaat dan niet alleen om de IT-componenten, maar ook om de verandering die Defensie met behulp van IT wil maken. Regie en integratie is dan een verantwoordelijkheid van Defensie én marktpartijen, die op basis van een goede taakverdeling en met kleine stapjes wordt gerealiseerd. De regie is het organiseren van vraag en aanbod. Enterprise architectuur, portfoliomanagement helpt daarbij, maar requirements management en verandermanagement ook. Het onderscheid tussen continuïteit en innovatie is niet altijd goed te maken, want soms is innovatie een integraal onderdeel van de af te nemen dienst of het voortdurende verandertraject. De detachering van personeel over en weer is een goede manier om kennis en ervaring uit te wisselen en beter samen op te trekken in de doorontwikkeling.

Tweede Workshop

De marktpartijen zijn van mening dat het noodzakelijk is dat Defensie zelf de regie voert. Zij kan zich daarbij door de marktpartijen en door de regiepartner laten ondersteunen. Maar ook bij de uitwerking van het High Level Ontwerp, in de architectuurfuncties en in het programmamanagement heeft Defensie zelf de eindregie op het organiseren van vraag en aanbod. Ze kan door middel van verschillende vormen van leveranciersoverleg een verwervingsvraag goed voorbereiden, een deel van het IT domein ten behoeve van de verwerving afbakenen en in beheersbare stappen laten uitvoeren. Zo kan Defensie de best practices van marktpartijen en andere opdrachtgevers optimaal benutten. Om dat te kunnen doen raden de marktpartijen Defensie aan te investeren in het eigen personeel, zowel ten behoeve van de regie als ten behoeve van continuïteit en innovatie. Inzet van personeel van Defensie bij marktpartijen is daarnaast goed mogelijk, zeker wanneer hun kennis actueel is en blijft.

4.3 Aandachtspunten en opmerkingen van marktpartijen

4.3.1 Eerste Workshop

Regierol en expertise markt

De marktpartijen zien regie als grip op de veranderaanpak en de inzet van IT en marktpartijen. Deze regie is niet tijdelijk, maar evolueert mee met de dynamiek van de vraag binnen Defensie en de capaciteit van de markt. Regie helpt vormgeven aan de inzet van marktpartijen. Deze inzet zou regie moeten vereenvoudigen als Defensie in staat is om de expertise van de marktpartijen goed te benutten. Dan kan er, afhankelijk van de aard van de vraag, de dienstverlening of het product, lichte of zware regie, strategische of meer operationele regie zijn. Regie is in ieder geval het organiseren van vraag en aanbod en meer dan alleen contractmanagement.

Regie vereist dat er overzicht is, en inzicht in de samenhang. Zowel aan de kant van Defensie als in de markt. Nu is voor de marktpartijen nog niet duidelijk hoe de besluitvorming en rollen ten behoeve van de bedrijfsprocessen binnen Defensie worden ingericht, bijvoorbeeld in de relatie tot de CDS en CIO. De marktpartijen zien de huidige inrichting als een risico om “best of breed” te gaan selecteren en integreren. De huidige documenten gaan vooral over IT, minder over (strategische) transformatie of veranderen en acceptatie door eindgebruikers. De marktpartijen stellen zich voor dat de regie door Defensie ook een teaminspanning is van Defensie en marktpartijen; dat beiden op basis van een gemeenschappelijk belang kunnen werken. De markt stelt hierbij dat de door hen gevraagde nadere uitwerking van (strategische) regievoering al onderdeel kan zijn van de te beginnen samenwerking. Daarbij is een aandachtspunt dat beide partijen ook zorgen voor continuïteit in de samenstelling van het ingezette team.

Meerdere leveranciers verschillende onderdelen

De marktpartijen willen graag de indeling van het IT domein ten behoeve van de verwerving nuanceren. Ze stellen voor dat er meer op diensten in plaats van op IT-onderdelen geselecteerd wordt. Bijvoorbeeld op type partijen en hun samenwerking met andere marktpartijen. Ook is flexibiliteit en dynamiek een belangrijk aandachtspunt; in deze voorgestelde aanpak gaat het meer om programmatisch dan projectmatig werken. Het betekent ook dat niet alles in een contract te regelen is en contractmanagement versterking behoeft om vorm aan de variatie in inzet van leveranciers te geven. De marktpartijen zelf zullen soms hun verdienmodel moeten aanpassen om binnen de voorgestelde condities te kunnen werken.

Personeel Defensie

De marktpartijen hebben in een aantal gevallen al ervaring met detachering van personeel over en weer. Het kan goed werken voor overdracht van kennis en ervaring over en weer. Er is wel een aantal randvoorwaarden. Zo moet duidelijk zijn onder wiens regie iemand op dat moment werkt (één baas), hoe service levels en betalingen geregeld worden, hoe je ervoor zorgt dat kennis gelijk blijft lopen tussen de partijen (certificeren) en de eventuele verandering in de eigen organisatie voldoende meemaakt.

Incrementele aanpak

De marktpartijen zien de incrementele aanpak niet als een bepaalde methodologie als Agile, maar als een groeipad met kleine stappen. Dus incrementeel is niet een implementatie per organisatie-onderdeel (dat is alles tegelijk voor die organisatie), maar eerder deel voor deel verwerven, en stukje voor stukje.

Onderscheid continuïteit en innovatie

Innovatie kan volgens de marktpartijen van continuïteit onderscheiden worden. Een innovatieteam van Defensie kan daarbij een goed instrument zijn (zie bijvoorbeeld bij de luchtmacht de Chief Innovation Officer). Aan de andere kant zijn continuïteit en innovatie vaak met elkaar verbonden. Om het applicatieportfolio te vernieuwen en door te ontwikkelen is ook de bestaande IT relevant. Zo zijn continuïteit en innovatie vaak beiden een onderdeel van de door te voeren transformatie.

Enterprise architectuur en Project Portfolio Management

De marktpartijen zijn van mening dat architectuur helpt bij regie over partnerships. Het is van belang de visie van Defensie daarin spoedig uit te werken, bijvoorbeeld samen met de markt, om als fundament voor de doorontwikkeling en de uitwerking van het samen-werkingsmodel te kunnen dienen. In die uitwerking is aandacht voor innovatie én

continuïteit gewenst, op een zodanige manier dat de regiefunctie er mee kan werken. In de huidige documenten is de Enterprise Architectuur en Project Portfolio Management nog te vaag en incompleet om goed regie te kunnen voeren. Andere in te zetten instrumenten zijn requirements management en verandermanagement.

4.3.2 Tweede Workshop

Regierol en expertise markt

De marktpartijen zijn van oordeel dat regie door Defensie moet; zij is in tegenstelling tot de marktpartijen in staat tot het organiseren van de interne vraagstelling en behoefte, het bepalen welke keuzen en afwegingen gemaakt moeten worden en het daarover verantwoording afleggen. Het is wel zaak dat Defensie daarvoor (uiteindelijk) zelf de expertise heeft en niet een externe partij selecteert om de andere externe partijen aan te sturen. In de huidige voorstellen is nog weinig aandacht voor het vanuit regie organiseren van de vraag en het voeren van regie over de delen van het IT domein ten behoeve van de verwerving heen.

De marktpartijen kunnen een zo groot mogelijke verantwoordelijkheid dragen onder regie van Defensie. De voorgestelde indeling van het IT domein ten behoeve van de verwerving maakt dat wel lastiger. Marktpartijen kunnen Defensie helpen de regierol te versterken en integratie te vereenvoudigen door behulpzaam te zijn bij het uitwerken van het High Level Ontwerp, het invullen van programmamanagement en het inrichten van een architectuur office. Daarbij raden marktpartijen aan om, door het gebruiken van algemeen bekende methodologieën, te zorgen voor gemeenschappelijk taalgebruik en afbakening van taken en verantwoordelijkheden. Met deze instrumenten kan een uitvraag scherper geformuleerd worden terwijl de integratie bewaakt wordt, en kan gemakkelijker getoetst worden of de doorontwikkeling op het gewenste pad ligt.

Meerdere leveranciers verschillende onderdelen

De marktpartijen geven aan dat de afbakening van onderdelen bepalend is voor de integratieproblematiek. Niet alleen voor de doorontwikkeling IT, maar ook in relatie met de bestaande IT. Het is van belang voor een goede inzet van marktpartijen dat zij inzicht hebben in het geheel. Het inrichten van een vorm van leveranciersoverleg is behulpzaam voor het delen van ontwikkelingen binnen Defensie en de markt en het kunnen afstemmen van vraag en aanbod.

De marktpartijen verwachten dat de indeling van het IT domein ten behoeve van de verwerving redelijk standaard (marktconform) kan zijn voor de statische IT, maar meer specifiek zal zijn voor de ontplooide IT. Zij wijzen erop dat dat onderscheid soms lastig te maken is als IT-componenten in beide situaties worden ingezet.

Personeel Defensie

Marktpartijen zien verschillende mogelijkheden om met Defensiepersoneel samen te werken, afhankelijk van wat Defensie ermee wil bereiken: leren van elkaar of samenwerken in bepaalde projecten voor een resultaat. Ze zien een risico in het verschil in kennisniveau tussen de innovatieve bedrijven en het in te zetten Defensiepersoneel.

Defensie zou volgens de marktpartijen moeten zorgen voor het behoud van IT-kennis en ervaring binnen de eigen organisatie om de eigen rol goed te kunnen vervullen. Daarvoor zijn passende loopbaanperspectieven, en minder doorstroom, wenselijk.

Incrementele aanpak

De marktpartijen ondersteunen de wens voor een incrementele aanpak. Beginnen met datacenter en werkplekken ligt daarbij voor de hand, hoewel het geen kleine stap is. Daarbij onderscheiden de marktpartijen wel een eerste oplevering en het verder uitrollen en in gebruik nemen ervan. Door de stap voor stap benadering kan Defensie, en de markt, ook leren van wat goed gaat en/of sneller kan. Het samen leren van de stappen zowel ten behoeve van de continuïteit als innovatie kan in de vorm van een gezamenlijk operationeel centrum waarin ontwerpers en beheerders een plaats hebben. De experts van Defensie en markt kunnen daarin samen probleemoplossend werken. Ze kunnen gebruik maken van ervaring die al elders is opgedaan, bijvoorbeeld bij de shared service centra van de overheid of de omgang met legacy in de industrie en financiële sector. Bijzondere aandachtspunten bij de incrementele aanpak zijn de doorlooptijd voor selectietrajecten en de omgang met tegenvallers.

Onderscheid continuïteit en innovatie

De marktpartijen wijzen erop dat continuïteit en innovatie met elkaar samenhangen. Er is veel innovatieve technologie beschikbaar, maar de vraag is wat realiseerbaar is binnen de situatie van Defensie. Daarbij is de vraag hoe Defensie om wil gaan met het onderscheid tussen het leveren van IT-diensten inclusief (technologische) innovatie versus het verwerven van IT in eigendom.

Enterprise architectuur en Project Portfolio Management

De marktpartijen zien architectuur en project- en programmamanagement als belangrijke, en noodzakelijke, instrumenten om regie te kunnen voeren.

5 Kunnen Defensie en markt tot passende afspraken komen?

5.1 De vraag van Defensie

Kan Defensie tot voor Defensie en marktpartijen passende prijsafspraken en contracten komen?

Waarbij Defensie streeft naar:

- Selectie van marktpartijen voor afgebakende onderdelen op basis van prijs/ prestatie, "cultural fit" en perspectief voor medewerkers;
- De afgebakende onderdelen zijn voldoende groot en marktconform en kennen een gefaseerd migratiepad;
- De samenwerkingsovereenkomst(en) kennen voldoende flexibiliteit t.b.v. toekomstige uitbreiding en/of innovatie;
- Een externe partij investeert in de nieuwe IT-infrastructuur en neemt dat op in de tarieven voor dienstverlening;
- Defensie onderscheidt continuïteit en innovatie in de contracten en budgetten;
- Defensie houdt zelf de overall regie, maar kan afgebakende onderdelen van Ontwikkelen en Beheren als resultaatopdracht aan marktpartijen gunnen.

De marktpartijen hebben deze vraag in drie groepen in aanwezigheid van vertegenwoordigers van Defensie besproken. Paragraaf 5.2 geeft een samenvatting van de bespreking. Paragraaf 5.3 geeft de aandachtspunten en opmerkingen van de marktpartijen in de vorm van korte alinea's weer.

5.2 Het samenvattende antwoord van de markt

Eerste workshop

De marktpartijen raden aan de selectie van leveranciers en de inhoud en het management van contracten goed aan te laten sluiten op de eisen vanuit regie. De aard en duur van de relatie met de leveranciers, het betrokken deel van het IT domein ten behoeve van de verwerving, de al dan niet daarin opgenomen vernieuwing en de in te zetten expertise bepalen de contractuele voorwaarden en prijsmodellen. Het samenwerkingsmodel stelt hoge eisen aan procurement. De marktpartijen raden dan ook aan daarin blijvend te investeren en meer gebruik te maken van de mogelijkheden die de aanbestedingswetten bieden om ook op inhoudelijke criteria te selecteren.

Tweede workshop

De marktpartijen zien op basis van hun ervaring met andere opdrachtgevers voldoende mogelijkheden om tot passende prijsafspraken en contracten te komen. Het vraagt wel een andere opstelling en kennis en expertise van Defensie zelf. In het bijzonder is het op basis

van passend vooroverleg komen tot een goede verwervingsvraag, selectiecriteria, service levels én selectiemethode van belang. Dan kunnen marktpartijen al dan niet als samenwerkingsverband ingaan op de verschillende aspecten als inzet van personeel van Defensie, prijsmodel, resultaatgerichtheid en het leveren van continuïteit én innovatie. De aanbestedingsprocedure moet echter wel worden aangepast, sneller en flexibeler, waardoor beter kan worden meebewogen met de snelle ontwikkeling van markt en technologie.

5.3 Aandachtspunten en opmerkingen van marktpartijen

5.3.1 Eerste Workshop

Selectie op basis prijs/prestatie, cultural fit en perspectief medewerkers

De marktpartijen hebben diverse opmerkingen bij de voorgestelde selectiecriteria. Zo is hun ervaring dat prijs vaak te zwaar gewogen wordt ten opzichte van kwaliteit. Om op kwaliteit te selecteren is een uitwerking per domein, niet per se de genoemde indeling ten behoeve van de verwerving zijnde, nodig. Er kunnen grote verschillen zijn tussen specialisten of grote leveranciers, al dan niet zichtbaar zijn van innovaties, transparantie van losse, horizontaal of verticaal geïntegreerde oplossingen, beschikbare capaciteit, enz. Veel aandacht is nodig voor de meetbaarheid van harde én zachte factoren. Zo geldt cultural fit ook voor partijen onderling, en niet alleen naar Defensie zelf. De inzet van mensen zou op basis van duidelijke doelen voor samenwerking moeten plaatsvinden, zoals het opereren in een IT-keten, kennisopbouw of kennismaking (stages, uitwisseling) en helderheid over de situatie op langere termijn (groei of krimp personeel).

Een dergelijke wijze van selecteren stelt ook eisen aan Defensie zelf, in het bijzonder inkoop- en contractmanagement, om te voorkomen dat het inkopen en selecteren voor alle betrokkenen niet aan de verwachtingen voldoet. De marktpartijen raden Defensie aan te investeren in voldoende eigen procurement expertise, niet eenmalig, maar als doorlopend proces.

Afgebakende onderdelen zijn voldoende groot en marktconform

De afbakening van onderdelen op grootte (geld) of duur van de relatie bepaalt mede het gedrag van de marktpartijen. Deze indeling is dus van groot belang. De marktpartijen verwachten dat Defensie zich verdiept in de business case van de leverancier en andersom. Het onderscheid tussen commodity diensten en specifieke oplossingen voor Defensie heeft daarbij invloed op omvang en marktconformiteit. Bij marktpartijen zijn ook

andere methoden bekend om voor een bepaald budget een specifieke oplossing te verwerven (Should Cost Management[2]).

Samenwerkingsovereenkomsten kennen voldoende flexibiliteit

De marktpartijen geven aan dat transparantie en duidelijkheid over en weer voorwaarden zijn voor passende samenwerkingsovereenkomsten. Flexibiliteit kan een onderdeel zijn van de samenwerking, bijvoorbeeld als over innovatie kengetallen met betrekking tot klantbinding zijn gemaakt. De vormgeving van de overeenkomsten is afhankelijk van de soort van relaties, van strategisch regiepartner tot uitvoerder. Let daarbij goed op het uitwerken van de grenzen tussen delen van het IT domein ten behoeve van de verwerving en/of leveranciers: de uitwerking bepaalt de kans op zand in de motor.

Investering IT infrastructuur opnemen in tarieven

Investering in infrastructuur in tarieven komt al vaker voor, bijvoorbeeld in de vorm van pay for use. Sommige marktpartijen denken dan ook niet meer in investeringen, maar in diensten die zij leveren. Andere door marktpartijen genoemde mogelijkheden zijn het mede afhankelijk laten zijn van de prijs van andere overheidsgebruikers en het gebruik van cloud diensten. Een belangrijke afweging voor Defensie is de make or buy beslissing voor infrastructuur.

Onderscheid innovatie en continuïteit in contracten en budgetten

De marktpartijen geven aan dat het zaak is contracten aan te laten sluiten op business principes (wat je echt belangrijk vindt) van betrokken partijen. Als dat voldoende transparant is, kunnen op basis daarvan betere afspraken gemaakt worden over innovatie, intellectual property, prijs en flexibiliteit. Zoals eerder aangegeven door marktpartijen kan in veel gevallen geen onderscheid worden gemaakt tussen innovatie en continuïteit, maar gaan deze hand in hand. Ook kan de vraag naar (business)innovatie vanuit Defensie verschillen van het IT-aanbod vanuit de markt. Het aanbestedingsrecht biedt volgens de marktpartijen meer mogelijkheden dan nu vaak benut.

Defensie houdt regie maar kan afgebakende onderdelen als resultaatopdracht inrichten

De marktpartijen zijn van mening dat binnen de regie ook resultaatopdrachten mogelijk zijn. Een en ander is afhankelijk van de eerder genoemde indeling van het IT domein ten behoeve van de verwerving en de aard van de relatie met de in te zetten leveranciers. Ook de eigen aanpak, programma- of projectmatig werken, speelt daarbij een rol. Om de

[2] Zie Should Cost Management, Why? How? Bij John Mueller, Undersecretary of Defense

marktpartijen goed te kunnen benutten in hun expertise is het van belang vertrouwen te kunnen geven. Contractmanagement is een onderdeel van regie en gaat ook in op de gewenste flexibiliteit en een exit strategie.

5.3.2 Tweede Workshop

Selectie op basis prijs/prestatie, cultural fit en perspectief medewerkers

De marktpartijen geven aan dat selectie niet op basis van één model van prijs/prestatie of cultural fit kan plaatsvinden. Een onderscheid naar commodity (standaard) of specialistische diensten is gewenst. Ook raden, zoals eerder aangegeven, marktpartijen aan meer functioneel uit te vragen. Dus niet (over) gespecificeerd op productkenmerken, maar meer op passendheid in gebruik. Cultural fit is daarbij niet alleen iets tussen Defensie en marktpartijen, maar ook tussen marktpartijen onderling. Cultural fit, maar ook het gewenste partnership of samenwerkingsmodel, kan maximaal benut worden als markt-partijen vooraf goed betrokken worden bij de vraagstelling, zodat Defensie en marktpartijen beter kunnen definiëren wat de fit zou moeten zijn.

Afgebakende onderdelen zijn voldoende groot en marktconform

De marktpartijen stellen voor dat Defensie een marktoriëntatie doet ter voorbereiding op het verwerven van afgebakende onderdelen. Afhankelijk van het onderwerp kunnen daarvoor verschillende vormen van vooroverleg, selectie en contractering ingericht worden; variërend van inkoop via Rijk tot Best Value Procurement. Het huidige High Level Ontwerp sluit niet optimaal aan bij de mogelijkheden in de markt, bijvoorbeeld ten aanzien van het lifecycle management van een IT-keten. De regiepartner kan helpen bij dit vooroverleg met de markt en het beoordelen van voor Defensie reële mogelijkheden van verwerving. Het biedt ook de gelegenheid oplossingsrichtingen te definiëren voor de inzet van verschillende soorten leveranciers, zowel voor Defensie bekende als nog onbekende leveranciers. De marktpartijen geven aan dat de ervaring leert dat deze tijdsinvestering vooraf bij de uitvoering ruimschoots wordt terugverdiend.

Samenwerkingsovereenkomsten kennen voldoende flexibiliteit

Om de samenwerkingsovereenkomsten voldoende flexibel te maken wijzen de markt-partijen op het belang van het vormgeven van de langere termijn commitment. Daarbij is het verdienmodel voor marktpartijen in relatie tot wat Defensie zowel meetbaar als zachter wil bereiken een aandachtspunt. Contracten zijn in de huidige vorm vaak te benauwend voor innovatie of omgang met veranderende omstandigheden of samenwerkings-verbanden. Ook de inzet van personeel van Defensie dient hierin een plek te krijgen. Het betekent wel dat de betrokken inkoop- en juridische afdelingen van Defensie meegroeien

in deze ontwikkeling en zelf innoveren. Het verder opbouwen en vasthouden van de noodzakelijke expertise is een belangrijk aandachtspunt.

Investering IT infrastructuur opnemen in tarieven

Er zijn verschillende bestaande mogelijkheden om investeringen in tarieven op te nemen. Zowel in de vorm van betaalde diensten als abonnementen. Om een passend model te kunnen kiezen, dienen Defensie en de marktpartijen voldoende te weten van elkaars kostenbepalende factoren. Zeker in het geval van meer innovatieve of voor Defensie specifieke diensten.

Onderscheid innovatie en continuïteit in contracten en budgetten

Het onderscheid tussen continuïteit en innovatie is volgens marktpartijen wel te maken, maar brengt wel een aantal risico's met zich mee. In de eerste plaats de blijvende aandacht voor innovatie en de financiering ervan. Maar ook dat continuïteit zonder innovatie steeds minder gebruikelijk is. Vernieuwing vindt meer en meer plaats gedurende het gebruik. En is daarmee een onderdeel van de te maken afspraken over beheer, met alle daarbij betrokken partijen voor de bestaande en nieuwe IT.

Bijzondere afspraken zijn nodig wanneer Defensie en marktpartijen samen investeren in een voor Defensie en markt nieuwe ontwikkeling. Zoals over intellectueel eigendom en het al dan niet kunnen inzetten voor andere opdrachtgevers van de ontwikkelde producten of diensten.

Defensie houdt regie maar kan afgebakende onderdelen als resultaatopdracht inrichten

Onder regie van Defensie is het goed mogelijk om afgebakende onderdelen resultaat-gericht aan één of meerdere marktpartijen uit te vragen. Het is volgens de marktpartijen dan wel van belang dat de regie, inkoop en juridische zaken van Defensie hierin goed samenwerken en hun expertise op dit gebied versterken.

6 Conclusies en aanbevelingen

Na de behandeling van de drie vragen van Defensie is de workshop afgesloten met samenvattende opmerkingen van alle marktpartijen en Defensie als opdrachtgever. De volgende paragrafen geven hiervan een overzicht, gesorteerd in een aantal onderwerpen.

6.1 Samenvattende opmerkingen van de marktpartijen

6.1.1 Eerste Workshop

Samenwerkingsmodel

Het samenwerkingsmodel maakt nog niet helemaal duidelijk wat Defensie van de marktpartijen verwacht. Schrijf helder op wat Defensie bedoelt en voer dit consistent door. Deze uitwerking kan al onderdeel zijn van de beoogde samenwerking. Daarmee is een eerste stap in open communicatie gezet. Het onderwerp is IT, maar het gaat om mensen van Defensie en marktpartijen. Dit samenwerkingsmodel vraag veel van vaardigheden met betrekking tot aanbesteden, regie en ketensamenwerking. Er is niet één samen-werkingsmodel; afhankelijk van het deel van de IT domein ten behoeve van de verwerving en de aard van de relatie kunnen bepaalde modellen ingezet worden.

Indeling van het IT domein ten behoeve van de verwerving

De voorgestelde indeling van het IT domein ten behoeve van de verwerving sluit niet goed aan bij wat er op de markt aanwezig is. Door wel goed aan te sluiten, ben je als Defensie des te flexibeler, bijvoorbeeld met COTS en open standaard producten. De indeling ten behoeve van de verwerving kan ook meer gebaseerd zijn op diensten en op wat in de cloud wereld gebruikelijk is. Maar blijf niet nadenken over deze indeling en steeds maar specificeren. Ga aan de slag met strategische partners.

Regie

Werk de visie van Defensie op de doorontwikkeling IT uit om de nog openstaande vragen te beantwoorden. Doe dit met de strategische partner. Kijk daarbij heel goed naar het regie- en governancemodel binnen Defensie. Werk deze uit. En bouw expertise op om te kunnen integreren en aan te sturen.

Zorg voor samenhang en continuous improvement in de doorontwikkeling. Houd de regie eenvoudig en eenduidig. Wees helder. Voorkom foutieve aannames. Optimaliseer de regie van Defensie zowel intern als richting markt.

6.1.2 Tweede Workshop

Samenwerkingsmodel

De marktpartijen zijn zeer positief over de dialoog die Defensie via deze ICT Haalbaarheidstoets met de markt voert. Zij raden Defensie dan ook aan met deze interactie door te gaan. Defensie en marktpartijen kunnen veel van elkaar leren. Deze openheid is ook tijdens de verwerving en contractering gewenst om de kennis en kunde van de markt te gebruiken en de samenwerking optimaal in te richten voor de gewenste stapsgewijze doorontwikkeling van de IT.

Indeling IT domein ten behoeve van de verwerving

De indeling van het IT domein ten behoeve van de verwerving is een belangrijk aandachtspunt. Het is nog de vraag of de nu voorgestelde afbakening van onderdelen optimaal is. Let op het onderscheid tussen de verschillende combinaties van IT-componenten voor Defensie bij definiëren van doelstellingen, service levels of resultaatafspraken met bijpassende prijsmodellen. Zorg er voor dat kleine beheersbare stappen gemaakt kunnen worden en dus dat de verwervingsvraag helder, duidelijk en pragmatisch is. Maak daarbij gebruik van wat elders bij de overheid of financiële wereld al geleerd is.

Regie

Regie op orde voor Defensie is hoogste prioriteit. Zorg vooral dat je weet wat je wilt en wat daarvoor nodig is. Accepteer dat deze verandering niet pijnloos of foutloos zal zijn. Maar richt je daarop in en wacht niet. Houd de eerste en volgende stappen simpel en haalbaar. Leer daarbij van anderen. In het bijzonder ook in de overgang van bestaande naar nieuwe IT.

6.2 Eerste bevindingen van Defensie uit de workshop

6.2.1 Eerste Workshop

Ron Kolkman, directeur JIVC, bedankt alle deelnemers voor hun inzet, tijd en openheid tijdens de workshop. Een aantal conclusies neemt hij aan het einde van de workshop al mee:

- Een aantal zaken mogen verder uitgewerkt voorafgaand aan verwerving
  - De regierol
  - Contractmanagement
  - High Level Ontwerp
- De samenwerking op langere termijn zou hard en zacht meetbaar moeten zijn
- De indeling van het IT domein ten behoeve van de verwerving is een belangrijk aandachtspunt
- Beveiliging kan zowel via de data als applicaties, data is wellicht eenvoudiger
- Should Cost Management als andere manier om tot nieuwe innovatieve oplossingen te komen
- Hoeveel geld is eigenlijk beschikbaar voor de doorontwikkeling IT?

6.2.2 Tweede Workshop

Ron Kolkman, directeur JIVC, bedankt alle deelnemers voor hun inzet, tijd en openheid tijdens de workshop. De aanbevelingen van vandaag zijn zeer waardevol en worden uiteraard door Defensie heel serieus genomen. Samenwerking en het hebben van een dialoog wordt zeer gewaardeerd en zinvol geacht. Het starten van de aanbesteding en contractering van de dienst Applicatie Housing en Hosting (groeikern) per 1 juli is een zeer ambitieus traject waar defensie en marktpartijen samen flink de schouders onder moeten zetten om het resultaat te bereiken. De ICT Haalbaarheidstoets is hiervoor een goede start. Defensie zal de markt blijven betrekken bij het ontwikkelen van de plannen.

Bijlage A Deelnemers ICT Haalbaarheidstoets

Deelnemers Eerste Workshop d.d. 12 juni 2015

Atos	Martin van Kesteren
BT Nederland N.V.	Marcel Kroeskop
Capgemini Nederland B.V.	Jasmijn Baldinger
CGI Nederland B.V.	Chris van Bronckhorst
Compumatica Secure Networks BV	Ad Koolen
Dell B.V.	Sandor Hazelhorst
Dimension Data Nederland B.V.	Edwin de Brave
EMC Federatie Nederland	Hans Timmerman
Hewlett-Packard Nederland B.V.	Bart Daniels
Hitachi Data Systems Nederland B.V.	Rob Hilterman
IBM Nederland B.V.	George van Duyneveldt
Juniper Networks International BV	Roberto Spadon
ITB-Kwadraat B.V.	Niels Hensen
KPMG Management Services B.V.	Hans Hopmans
Microsoft B.V.	Peter Beijderwellen
Ministerie van Defensie	Ari Nagtegaal
Ministerie van Defensie	Ron Kolkman
Ministerie van Defensie	Jean Paul Duckers
Ministerie van Defensie	Ronald Rietbergen
Ministerie van Defensie	Lebna de Voogd
Ministerie van Defensie	Tanja van Burgel

Ministerie van Defensie	Peter de Haas
Ministerie van Defensie	Marion Vos
Ministerie van Defensie	Jacques Snel
Misco Solutions B.V.	Patrick Laurier
Nederland ICT	Liesbeth Holterman
Nederland ICT	Floor Lekkerkerker
Ordina Nederland B.V.	Maas Bos
PBLQ	Jan van Veenen
PBLQ	Jan van der Burg
PBLQ	Evert-Jan Mulder
Software AG Nederland B.V.	Paul van de Waal
SYSQA BV	Johan Zandhuis
The Boston Consulting Group	Miel Geleijns
Unisys Nederland N.V.	Guido de Nobel
VMware Netherlands B.V.	Art de Blaauw
Xerox (Nederland) B.V.	Rob Muller

Deelnemers Tweede Workshop d.d. 26 juni 2015

Accenture	Jeroen Louman
Centric Netherlands B.V.	Paul de Vries
Cisco Systems International B.V.	Koen Bastiaens
Contour Advanced Systems B.V.	Wim Tijsterman
CSC Computer Sciences BV	Mark van Dijk
Deloitte Consulting B.V.	Marloes van de Braak
Everest	Tess Rutgers van Rozenburg
Fox-IT	Jeff Collée
i3 groep	Marc Borlee
KPN IT Solutions	Manuel Mentink
Ministerie van Defensie	Ari Nagtegaal
Ministerie van Defensie	Ron Kolkman
Ministerie van Defensie	Lex van der Loo
Ministerie van Defensie	Peter de Haas
Ministerie van Defensie	Marion Vos
Ministerie van Defensie	Ton van der Sanden
Nederland ICT	Liesbeth Holterman
Nederland ICT	Floor Lekkerkerker
NIDV	Ron Nulkes
Onsight Solutions	Obbe van Ommeren
OpenText	Ron Matser
Oracle Nederland B.V.	Maurice Godschalk
PBLQ	Jan van der Burg

PBLQ	Evert-Jan Mulder
PBLQ	Jan van Veenen
Pegasystems B.V.	Jan Willem Boissevain
PQR B.V.	Robert Verzaal
Protinus IT B.V.	Marcel Nulden
Red Hat	Koen van Bakel
SAP Nederland B.V.	Johan van Klinken
SAS Nederland	André van der Meer
Schuberg Philis	Mark Ostendorf
Sogeti Nederland B.V.	Sander Boerema
SQNetworks	Marco van Vliet
Vodafone Libertel B.V.	Andreas Stribos

Bijlage B Samenvatting High Level Ontwerp

Behorend bij ICT Haalbaarheidstoets d.d. 12 juni 2015.

1. Opzet en reikwijdte High Level IT Ontwerp (HLO)

Het doel van het HLO is om ambitie en richting te geven aan de inrichting van de toekomstige IT van Defensie. Het HLO is als het ware een stedenbouwkundig plan voor de doorontwikkelingsrichting van onze IT. Daarmee beschrijft het HLO niet in detail hoe onze IT in circa vijf jaar er uit zal zien en welk financieel beslag dat met zich mee brengt. In lijn met de bevindingen van de commissie Elias, wordt daarmee gekozen voor een incrementele aanpak. Belangrijk uitgangspunt in deze aanpak is dat IT nooit af zal zijn en aan de hand van actuele ontwikkelingen steeds zal moeten worden vernieuwd. In de voorgestelde aanpak worden steeds onderdelen uit het HLO nader uitgewerkt met bijbehorend eisenpakket inclusief financieel beslag. Bij iedere detaillering is een keuzemoment aan de orde. Deze aanpak is samengevat als: *think big, act small!* Defensie zal het HLO in samenwerking met de markt realiseren.

- *Uitgangspunten HLO.*

  Uitgangspunt voor het HLO is dat moderne IT cruciaal is voor het effectief en doelmatig functioneren van de krijgsmacht bij het ondersteunen van de commandovoering, de operationele inzet, de bemande en onbemande wapensystemen, de inlichtingen, de communicatiemiddelen en de bedrijfsprocessen. De krijgsmacht maakt onderdeel uit van een informatiemaatschappij die wordt gedreven door razendsnelle ontwikkelingen in de IT.

  Een nieuwe IT-infrastructuur moet een betrouwbare technische basis voor de IT van onze krijgsmacht opleveren en tegelijkertijd de weg openen naar de invoering van moderne technologieën zoals: cloudoplossingen, virtualisatie en het aansluiten op internationale, NATO-, rijks- en marktconforme standaarden. Dit stelt de krijgsmacht in staat veel eenvoudiger, sneller, efficiënter en vooral effectiever samen te werken met haar partners.

  Ook voor de toepassingen in de IT ontstaan nieuwe mogelijkheden. De huidige toepassingen zijn grotendeels gebaseerd op verouderde technologieën terwijl de moderne IT inmiddels veel flexibelere toepassingen biedt. Ten slotte creëert de modernisering van de IT-infrastructuur een momentum om te starten met een platform voor innovatie van IT binnen Defensie. Oftewel: een slimme combinatie van een nieuw platform en kennis vanuit Defensie, markt en partners, om IT in te zetten als permanente *enabler* voor de innovatie van de krijgsmacht als geheel.

  Het HLO biedt focus in de ontwikkeling van een modern en geïntegreerd IT-domein voor Defensie. Het ontwerp is gebaseerd op een inventarisatie van de ontwikkelingen in het militair optreden en de bedrijfsvoering, de staat van de huidige IT en de opzet van integraal *Business Continuity Management* (BCM). Het HLO beschrijft de effecten die IT in het militair optreden en de bedrijfsvoering moet bewerkstelligen of ondersteunen en

welke veranderrichting daarvoor nodig is. Dit is vertaald in kaders voor de toekomstige IT en principes voor de verandering. Het HLO is de weg waarlangs de IT van de krijgsmacht zich ontwikkelt richting de stip op de horizon die in de visie is neergezet.

- *Fundament HLO: de bedrijfsvoeringseisen en effecten.*

  De toekomstige rol van IT is het optimaal ondersteunen van de *eisen* vanuit de bedrijfsvoering:

  ✓ Bedrijfsvoering en de mens staan centraal, de IT sluit aan.
  ✓ De IT maakt veilig samenwerken in snel wisselende verbanden mogelijk.
  ✓ De IT is betrouwbaar en beschikbaar.
  ✓ Met de IT is Defensie wereldwijd *connected*.
  ✓ De IT is geschikt voor verwerken, opslaan en analyseren van zeer grote hoeveelheden informatie.
  ✓ De IT is eenvoudig en snel aanpasbaar.

  Op basis van deze eisen is bepaald wat Defensie wil bereiken met haar IT: dit zijn de *effecten*. Op basis van deze effecten zijn de globale eisen aan de IT uitgewerkt. Deze eisen staan niet op zichzelf maar worden ingegeven door overkoepelende trends in de informatiemaatschappij, de defensie-industrie en de behoefte om netwerkend op te treden. Tevens moet onze toekomstige IT voldoen aan de pijlers continuïteit, beveiliging en innovatie conform de visie op de IT.

  Het realiseren van een moderne IT die voldoet aan de eisen van de toekomst vraagt om verschillende ingrepen. Enerzijds is modernisering nodig van de IT-infrastructuur en anderzijds moet het huidige complexe landschap van IT-toepassingen (applicaties) ingrijpend worden gemoderniseerd. Het huidige IT-landschap wordt gekenmerkt door een grote diversiteit in technologie, sterk uiteenlopende levenscycli van IT-toepassingen (mix van moderne en verouderde toepassingen) en een gebrek aan veranderbaarheid (inflexibel). De IT-architectuur van Defensie is derhalve onvoldoende aangepast aan de veranderende eisen.

- *Verander- en migratieprincipes HLO.*

  In het HLO zijn de IT-infrastructuur en IT-toepassingen gesplitst. Deze zijn beide vanuit het pakket aan bedrijfsvoeringseisen uitgewerkt. Vervolgens zijn de volgende verander- en migratieprincipes benoemd:

  ✓ Naast de huidige IT-infrastructuur wordt een nieuwe infrastructuur ingericht. De huidige structuur blijft vooralsnog intact. Deze situatie duurt zo kort mogelijk, zolang als nodig. Op de huidige infrastructuur zijn - voor zover noodzakelijk – de huidige IT-toepassingen beschikbaar.
  ✓ De rationalisatie van IT-toepassingen vindt plaats langs de lijn van het verlagen van de TCO (*Total Cost of Ownership*), de reductie van de complexiteit, het verhogen van de beheersbaarheid en tot slot een kortere *time to market* van aanpassingen en nieuwe applicaties (apps).

De huidige IT-toepassingen worden overgezet naar de nieuwe IT-infrastructuur dan wel uitgefaseerd. Hiervoor wordt de volgende aanpak gebruikt:

- ✓ *FREEZE* (IT-toepassingen, tot moment uitfaseren, in de huidige vorm handhaven in de huidige IT-infrastructuur).
- ✓ *KILL* (met voorrang uitfaseren omdat het technisch of economisch niet rendabel is dit systeem in stand te houden).
- ✓ *ELU* (een *End-Life Update* geven en de levenscyclus in de legacy omgeving laten aflopen).
- ✓ *MIGRATE* (als *workload* gevirtualiseerd overbrengen naar de nieuwe IT-infrastructuur).
- ✓ *REBUILD* (vergelijkbare functionaliteit opnieuw inrichten).

Voor (COTS/NOTS) toepassingen zullen aanbieders op termijn huidige applicaties met een beproefde *upgrade* geschikt maken voor de nieuwe IT-infrastructuur.

- ✓ De nieuwe infrastructuur is de basis voor de gemoderniseerde IT. De gemoderniseerde IT is een groeikern en vervangt niet in één keer de huidige IT-infrastructuur en alle IT-toepassingen. De groeikern neemt gefaseerd de bestaande IT over en verandert mee met de behoeften van de krijgsmacht. De bestaande IT blijft gedurende deze migratie in gebruik om daar waar vereist nog steeds de processen binnen Defensie te ondersteunen (tot en met de operationele inzet). Kaders worden geformuleerd om onze processen te vereenvoudigen en daarmee ook het bestand aan bestaande IT-applicaties portfolio te rationaliseren langs de lijn van verlagen van de TCO (*Total Cost of Ownership*), reductie complexiteit en verhogen beheersbaarheid en tot slot een kortere *time to market* van aanpassingen en nieuwe applicaties (apps).
- ✓ Nieuwe toepassingen worden direct op de nieuwe infrastructuur ontwikkeld (zoals de moderne werkplekomgeving). De nieuwe infrastructuur vervult tevens de rol van innovatie- en integratiedomein en beproevingsomgeving. De gebruiker werkt in principe vanuit de nieuwe IT-infrastructuur, die in staat is om waar nodig applicaties en data uit de huidige IT-infrastructuur aan te roepen. Dit moet de bruikbaarheid en gebruikersvriendelijkheid, ook van de huidige applicaties, verbeteren.
- ✓ De IT-toepassingen worden zoveel als mogelijk onzichtbaar voor de gebruikers. Niet de toepassingen maar de informatiebehoefte komt centraal te staan. De nieuwe IT bevat voorzieningen om deze uniform toegankelijk te maken, afgestemd op rol, taak of functie.
- ✓ Het nieuwe IT-domein van de krijgsmacht wordt met generieke componenten ingericht. Dat gaat sneller en zekerder omdat deze componenten zijn beproefd en daardoor minder fouten kennen. Deze aanpak houdt in dat Defensie voor dit deel van haar domein niet zelf ontwikkelt. Voor het invullen van specifieke eisen vanuit het operationele domein ontwikkelt Defensie nog steeds zelf. Reden is dat de markt geen passende oplossing kan bieden of niet kan voldoen aan bepaalde eisen vanuit de criteria beschikbaarheid dan wel betrouwbaarheid. Daarom blijft eigen innovatie- en ontwikkelcapaciteit in stand.
- ✓ Door het HLO leidend te verklaren wordt voorkomen dat in het nieuwe domein de "huidige situatie" als vanzelfsprekend wordt geautomatiseerd. Met het HLO worden

nieuwe wegen ingeslagen. Iedere vernieuwing moet ook modernisering mogelijk maken.

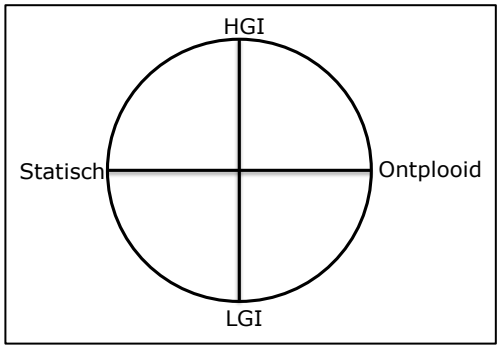
- ✓ Het HLO is als architectuur zoveel als mogelijk ontkoppeld van de organisatie-inrichting. Dit betekent dat veranderingen van de organisatie niet direct leiden tot verandering van de architectuur inclusief het applicatielandschap en de infrastructuur. Het is de uitdaging om in de komende jaren de ontkoppelpunten verder te expliciteren in zowel de processen als de output van de krijgsmacht. De nieuwe IT wordt opgezet op basis van bouwstenen en kent daardoor een modulaire opbouw, waardoor de flexibiliteit en aanpassingsvermogen hoog zijn.
- ✓ De toenemende behoefte aan samenwerking vereist meer koppelingen terwijl de cyberdreigingen toenemen. Om de informatiebeveiliging te borgen, vereist dit het continu blijven ontwikkelen en verbeteren van de beveiligingsmaatregelen. Hiermee blijven koppelingen met derden mogelijk inclusief functionele verbetering, terwijl de risico's inzichtelijk en beheersbaar zijn. Dit vereist een verschuiving van netwerkbeveiliging naar beveiliging van de informatie.
- ✓ Medewerkers krijgen de middelen om IT optimaal te benutten in de vorm van een digitale uitrusting.

2. Samenwerking met de markt is noodzakelijk

Defensie heeft geconcludeerd dat zij de markt nodig heeft om haar IT-diensten te kunnen leveren. In het HLO is vastgesteld dat Defensie haar IT-activiteiten altijd onder eigen verantwoordelijkheid (regie) zal uitvoeren vanwege de indringende relatie van IT met haar unieke primaire taak. Voor het uitwerken van de wijze waarop met de markt wordt samengewerkt zijn varianten als "zelf doen", "samenwerken" en "uitbesteden" de revue gepasseerd. Om de snelheid en flexibiliteit van samenwerking met marktpartijen in de volle breedte te benutten is gekozen voor partnerships waarbij intensief wordt samengewerkt met marktpartijen. In deze samenwerkingsvorm gaat geen personeel van Defensie over naar de markt. Bij deze samenwerkingsverbanden zal Defensie altijd moeten aanbesteden door middel van de geëigende (Europese) aanbestedingsprocedure (uitzonderingsbepalingen in de Defensiewet daargelaten).

Onderstaande opsomming bevat de generieke karakteristieken van het voorgestelde samenwerkingsmodel. Afwijkingen op deze karakteristieken per service zijn mogelijk, maar worden apart gespecificeerd.

- ✓ De strategische samenwerking van Defensie met de markt betreft de nieuwe IT. Hierbij worden de IT-activiteiten langs de assen Statisch-Ontplooid en Laag Gerubriceerde Informatie (LGI) – Hoog Gerubriceerde Informatie (HGI) ingedeeld (zie onderstaand figuur en bijlage 2 voor toelichting termen).



Figuur 1. Onderverdeling IT-domein Defensie

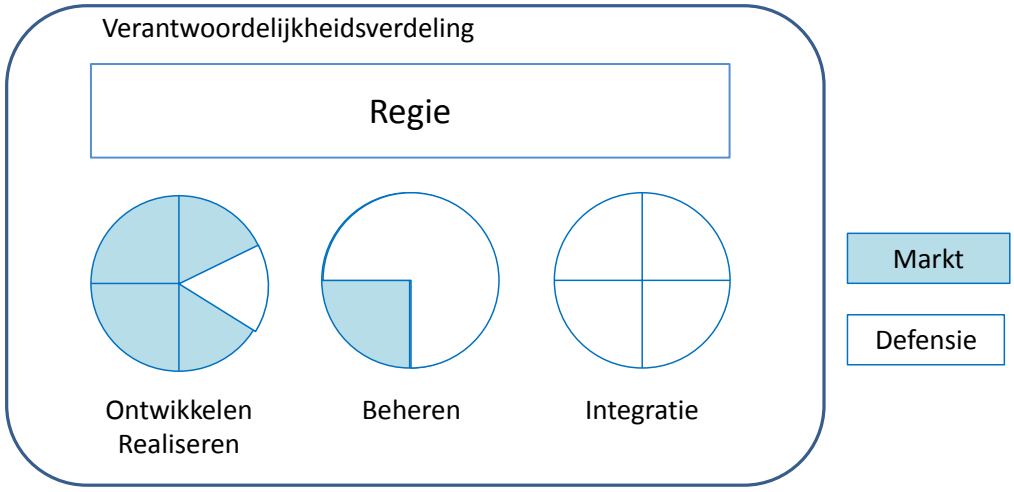
(In de figuren 2 en 3 is voor de "bollen" dezelfde indeling als in figuur 2 gebruikt.)

- ✓ Defensie kiest voor meerdere partijen (*best of breed*) voor de nieuwe IT welke niet alleen worden geselecteerd op basis van prijs/prestatie, maar ook op basis van 'cultural fit' en perspectief voor medewerkers.
- ✓ De samenwerking vindt niet plaats in een aparte juridische entiteit[3].
- ✓ De samenwerking met de markt geschiedt gefaseerd in afgebakende onderdelen die voldoende groot zijn voor marktpartijen alsook marktconform en beheersbaar zijn, waarbij rekening wordt gehouden met het absorptievermogen van de uitvoeringsorganisatie. Hierbij wordt vooralsnog de indeling van services uit hoofdstuk 3 gehanteerd.
- ✓ De huidige IT-infrastructuur blijft nog een aantal jaar operationeel onder verantwoordelijkheid van Defensie. Hiervoor kunnen externe partijen worden ingezet (zoals nu ook al het geval is).
- ✓ Defensie behoudt zelf de regie- en integratiefunctie[4] (inclusief technische expertise) en laat zich hierbij ondersteunen door een externe strategische partner.
- ✓ De samenwerkingsaanpak brengt met zich mee dat Defensie de (integrale) eindverantwoordelijkheid houdt over de IT-infrastructuur.

De verantwoordelijkheidsverdeling is conform het rapport 'Grensverleggende IT' als volgt bepaald (de uitvoering van activiteiten kan anders worden belegd).

3 Conform het kabinetsbeleid dat uiterst restrictief is met betrekking tot deelnemingen. Alleen in uiterste noodzaak, als geen alternatief voorhanden is, kan een deelneming nog een oplossing zijn. Bron: MinFin

4 Technische integratie van diensten wordt zoveel mogelijk bij externe partij(en) belegd. Technische integratie van wapensystemen blijft bij Defensie belegd.



Figuur 2. Verantwoordelijkheidsverdeling Defensie en markt

Samenwerken met de markt lukt alleen wanneer er een duidelijke verant-woordelijkheidsverdeling is. Wanneer die ontbreekt of onduidelijk is, dan zal de opdrachtgever vrijwel altijd de volledige verantwoordelijkheid dragen. Daarom is bij de verdeling van de verant-woordelijkheden tussen Defensie en markt gekozen voor onderstaande indeling.

Verantwoordelijkheid voor:	Ontwikkelen & Realiseren:	Beheren:	Integreren (regie):
HGI	Markt/Defensie)*	Defensie	Defensie
LGI – statisch	Markt	Markt	Defensie
LGI – ontplooid	Markt/Defensie	Defensie	Defensie

)*: voor een bepaald deel zal gelden dat Defensie verantwoordelijk is.

De exacte inhoud van de "taartpunten" (de IT-objecten en IT-activiteiten) worden bepaald door middel van de vijf scope criteria uit het HLO:

- Het object of de activiteit is niet overdraagbaar.
- De activiteit betreft instandhouding van een hoog gerubriceerd object.
- De activiteit wordt uitgevoerd onder ontplooide omstandigheden.
- De activiteit betreft essentiële regievoering.
- Het is een erkende uitzondering.

✓ Binnen de verantwoordelijkheidsverdeling worden activiteiten door de externe partijen en Defensie gezamenlijk uitgevoerd binnen de regels en kaders van de

verantwoordelijke. De condities waaronder deze inzet plaats vindt moet nader worden uitgewerkt. Defensiepersoneel blijft bij Defensie, maar wordt voor zover nodig ingezet, bij IT-activiteiten die onder verantwoordelijkheid van de markt worden gebracht. Voor een klein specifiek deel zal gelden dat Defensie zelf ontwikkelt en realiseert.

- ✓ Eigenaarschap middelen (hardware en software) is belegd bij de markt (in ieder geval voor LGI met uitzondering van C2-systemen, voor HGI moet dit nader worden uitgezocht). Sommige software contracten kunnen niet worden overgedragen. Terugname mogelijkheid van middelen moet gegarandeerd zijn.
- ✓ Het *Wide Area Netwerk* (WAN[5]) is van vitaal belang voor de bedrijfsvoering van Defensie[6]. Defensie hanteert voor het WAN specifieke ontwerpprincipes, zoals een sterk beveiligd koppelvlak (genaamd IEGI) naar externe netwerken. Vanwege het specifieke karakter en de aanmerking als vitale infrastructuur blijft het WAN binnen Defensie en is samenwerking met andere partijen binnen de Rijksoverheid het best passend voor een strategische asset als het WAN.
- ✓ De externe partij investeert in de nieuwe IT-infrastructuur. De kosten worden opgenomen in de tarieven van de dienstverlening. Betaling van deze partijen vindt plaats op basis van afgesproken prestaties per dienstverlening (zoals SAAS). Dit wordt uitgewerkt in de aanbestedingsstrategie.
- ✓ De samenwerkingsovereenkomst moet voldoende flexibiliteit bezitten om toekomstige dienstverlening (groeikern) te kunnen absorberen. Defensie neemt op basis van behoefte in de tijd diensten af (flexibiliteit) op basis van nadere overeenkomsten binnen de samenwerkingsovereenkomst.
- ✓ Het stimuleren van de innovatie bij en door externe partijen moet een bewust onderdeel zijn van de samenwerking. Dit wordt ingevuld door:
  - Spanning tussen continuïteit en innovatie niet in één contract onder te brengen. Innovatie wordt apart benoemd met een separaat contract.
  - De mogelijkheden om binnen Defensie naar eigen keuze en eigen wensen innovatieve initiatieven te ontplooien met derden worden zeker gesteld.
  - Een nader vast te stellen innovatiebudget wordt gereserveerd met bij aanwending financiële middelen afspraken over *time to market*.
- ✓ De vastgestelde beveiligingseisen moeten in overeenstemming met de Defensiewet worden toegepast. Voor vitale infrastructuur kan het noodzakelijk zijn om gebruik te maken van de uitzonderingsbepalingen in de Defensiewet.
- ✓ Defensie moet de mogelijkheid hebben om in een last resort situatie haar IT zelf te kunnen beheren. Daartoe kan Defensie te allen tijde de dienstverlening van de

5 Onder het WAN wordt verstaan het NAFIN (glasvezelnetwerk van Defensie) inclusief de netwerklagen die daarop zijn gerealiseerd (tot aan het koppelvlak met de bekabeling in gebouwen). Dit is inclusief de huurlijnen die worden gebruikt voor het koppelen van locaties waar geen NAFIN is. Het juridisch eigendom van NAFIN ligt op de markt.

6 Het WAN is niet alleen vitaal voor de bedrijfsvoering van Defensie, maar is door een besluit van de staatssecretaris van Economische Zaken op 14 januari 2008 (nr. ET/TM/7135438) op grond van artikel 5.16 van de Telecommunicatiewet ook aangewezen als elektronisch communicatienetwerk dat geheel of hoofdzakelijk gebruikt wordt voor vitale overheidstaken.

markt terugnemen, de voorwaarden en condities waaronder dit gebeurt, moeten worden uitgewerkt.

3. Personeel heeft perspectief

Het personeel wordt binnen dit scenario niet naar buiten geplaatst, het blijft bij Defensie. Echter wanneer de transitie naar de nieuwe IT wordt uitgevoerd conform het HLO dan zal dit consequenties hebben voor het personeel. De ervaringen in de markt laten zien dat voor de nieuwe IT minder personeel en personeel met andere skills nodig is.

Dit heeft consequenties voor de inrichting van de IT-keten binnen Defensie, minder benodigde aantal medewerkers en andere kennis/kunde en competenties van het personeel (dit zal leiden tot reorganisatietrajecten). Er is voldoende perspectief voor het huidige personeel. Binnen de constructie van samenwerken met de markt heeft het personeel perspectief op tenminste de volgende gebieden:

- ✓ Beheren van HGI zal altijd door Defensie worden uitgevoerd.
- ✓ Beheren van huidige omgeving zal nog enige jaren voortduren.
- ✓ Samen beheren van nieuwe omgeving LGI met externe partij.
- ✓ Regie is cruciale rol die bij Defensie blijft.

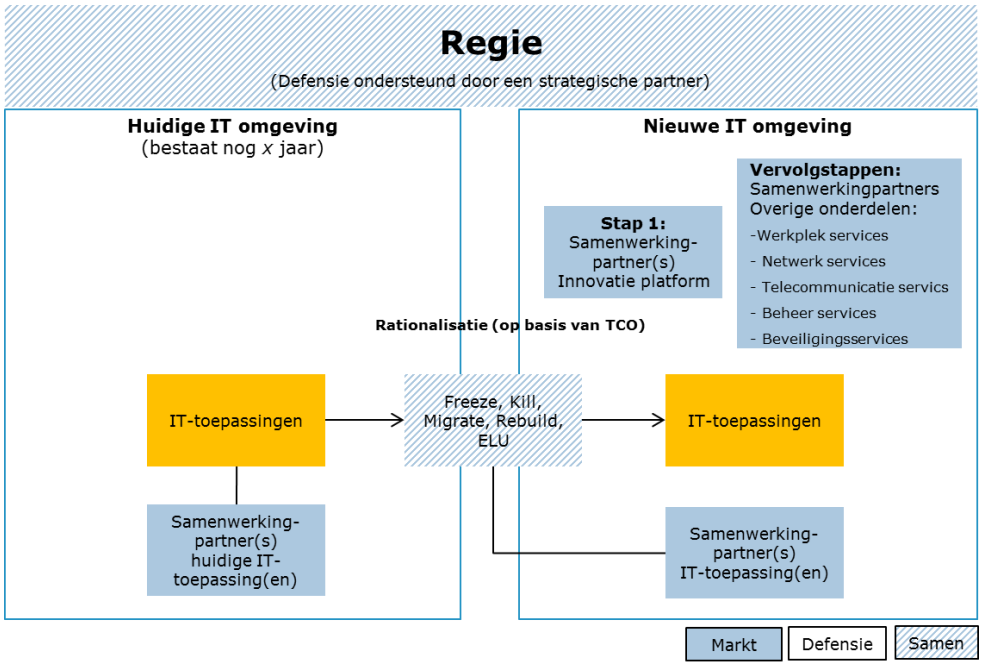
4. Regie is cruciaal voor een succesvolle samenwerking

Regie is essentieel bij vernieuwing en modernisering. Aansturing van leveranciers, coördinatie en sturing van de migratie-activiteiten en specificeren wat verwacht wordt van externe partijen is essentieel. Tevens dient aandacht te zijn voor monitoring, review en audit mogelijkheden (rapport Elias).

Als onderdeel van de IT-regie moet de IT-strategie, *Enterprise* architectuur (met als basis het HLO) en *governance* verder worden ontwikkeld en uitgewerkt. Daarnaast moeten op uitvoerend niveau meerdere externe partijen worden aangestuurd in combinatie met een deel van de dienstverlening die door Defensie zelf wordt uitgevoerd. Op centraal niveau binnen Defensie is de verantwoordelijkheid belegd voor het in balans brengen van de behoeftes, middelen en de beschikbare capaciteit met Project Portfolio Management (PPM) als instrument. Binnen dit hele spectrum is het aanbrengen en bewaken van de integraliteit noodzakelijk. Bij alle activiteiten is een diepgaande en excellente samenwerking tussen de verschillende directies binnen Defensie een vereiste.

Het versnellen en versterken van regie door ondersteuning van een externe strategische partner wordt daarom als cruciale succesfactor gezien. Hierbij gelden de volgende uitgangspunten:

- ✓ Defensie blijft zelf “de” regieorganisatie en stuurt deze ook zelf actief aan.
- ✓ Externe strategische partner versterkt Defensie in haar rol.



Figuur 3. Regie IT-domein met een externe strategische partner

- ✓ De scope van de strategisch partner is: het uitwerken van het HLO, advisering bij migratie IT-toepassingen, advisering opzet en samenwerking met de markt, advisering bij continuïteit van de huidige omgeving, *quality assurance* en *risk management*, het ondersteunen bij doorontwikkelen en professionaliseren regieorganisatie en het inregelen van de integratie. Waar mogelijk zullen regietaken ook betrokken worden uit de staande organisatie.
- ✓ De externe strategische partner zal niet in de uitvoering zitten.

Deze aanpak wordt in figuur 3 verduidelijkt.

5. Stapsgewijze realisatie HLO

Het HLO als stedenbouwkundig plan wordt uitgewerkt in stappen. Deze stappen geven aan hoe het HLO tot uitvoering wordt gebracht. De stappen zijn incrementeel en imperatief; er kan worden bijgestuurd zodat de stappen blijven aansluiten op de prioriteiten, beschikbare middelen en beste oplossingsmogelijkheden. De volgorde en inhoud van de stappen wordt als volgt bepaald:

- Op de huidige IT-infrastructuur vinden alleen investeringen dan wel "updates en upgrades" plaats om risico's voor discontinuïteit in militair optreden en/of bedrijfsvoering te voorkomen of omdat Defensie gehouden is aan wetgeving.
- Waar strikt noodzakelijk hebben "updates en upgrades" voorrang op vernieuwing.
- Eerst focus op randvoorwaardelijke IT-bouwblokken en daarna op het bereiken van business effecten.
- IT-infrastructuur voor militaire operaties en inlichtingen hebben voorrang op de overige delen van de IT-infrastructuur.

- Doel is één Defensie IT-infrastructuur. Dit wordt niet in één keer gerealiseerd maar in kort cyclische projecten (met als uitgangspunt een maximale doorlooptijd per project van één jaar).

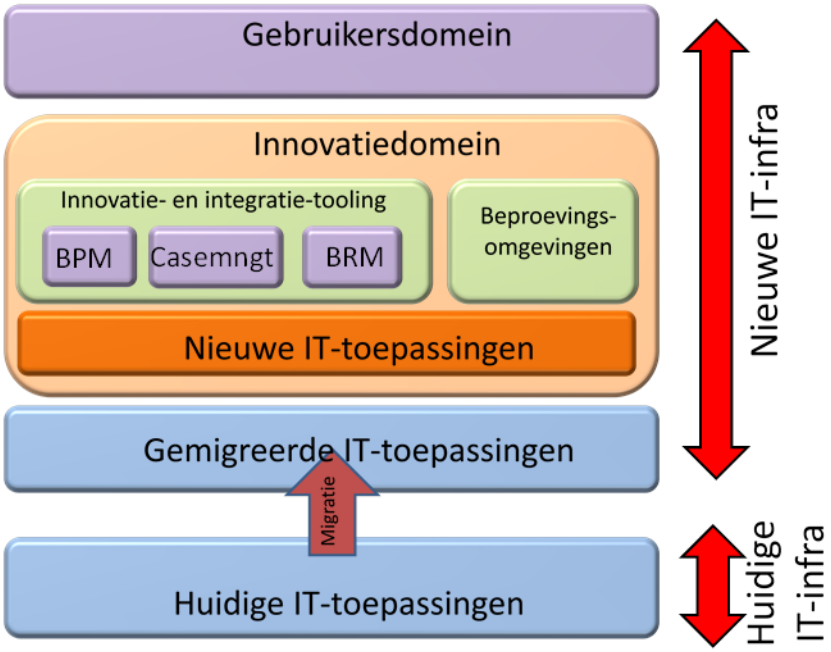
De eerste stap in de realisatie van het HLO omvat de inrichting van een gemoderniseerde basis IT-infrastructuur. Deze nieuwe IT-infrastructuur is een technische omgeving die geschikt is voor twee doelen:

- De technische basis voor het innovatieplatform (de nieuw te ontwikkelen IT van Defensie);
- De technische basis voor bestaande systemen die volgens de rationalisatiemethodiek worden geselecteerd om te migreren (de te behouden huidige IT van Defensie die migreert).

De nieuwe IT-infrastructuur is dus meer dan het innovatieplatform. Het innovatieplatform is gericht op de IT van de toekomst terwijl de nieuwe IT-infrastructuur ook bestaande IT gaat ondersteunen die nog langjarig binnen Defensie gebruikt wordt en voldoet aan de criteria om te kunnen migreren.

De nieuwe infrastructuur ontwikkelt zich vanuit het groeikern-principe. Dit is een manier van ontwikkelen waarbij kleinschalig wordt gestart, echter zodanig wordt vormgegeven, dat snel en flexibel kan worden opgeschaald. De groeikern staat dus voor een werkwijze waarop de nieuwe IT-infra zich gaat ontwikkelen met de behoefte van Defensie.

De nieuwe IT-infra valt daarmee uiteen in twee technische architectuursegmenten, namelijk het segment voor het innovatieplatform en het segment voor gemigreerde toepassingen die nog op oudere architectuurconcepten gebaseerd zijn, maar wel nog langjarig binnen Defensie gebruikt gaan worden en waarvan het niet wenselijk is dat deze op de huidige IT-infrastructuur blijven. Voor beide segmenten geldt doorgaans een ander beheerregime en is andere kennis vereist.



Figuur 4. Rationalisatiemethodiek

De continuïteit van de huidige IT-dienstverlening heeft de hoogste prioriteit. Uit het IT-assessment is naar voren gekomen dat bij de Datacenters de grootste knelpunten en issues zijn. De applicatie housing en hosting (AHH) wordt als dienst aanbesteed waarbij de verantwoordelijkheidsverdeling en de uitvoering van het beheer zoals beschreven in het HLO als uitgangspunt geldt (zie figuur 2 en 3). De scope is het ontwikkelen en realiseren van een groeikern LGI en HGI (statisch en ontplooid). De marktpartij neemt hier verantwoordelijkheid voor:

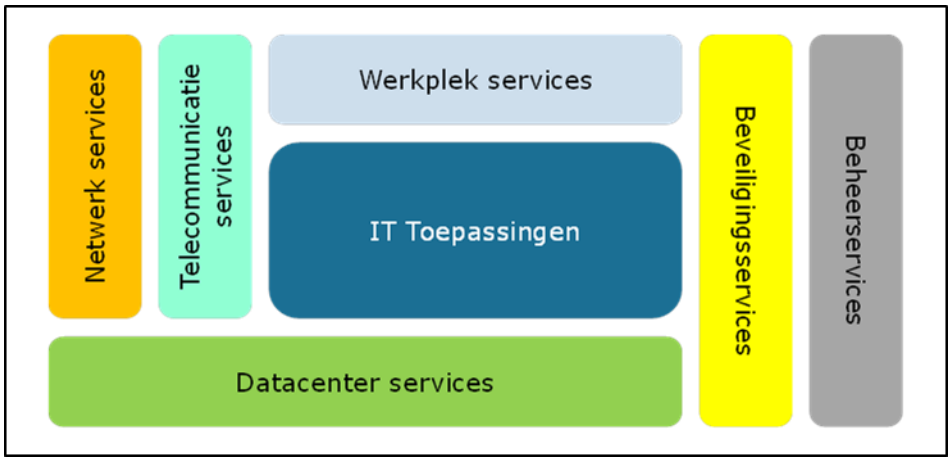
- Het ontwerp en realisatie (LGI/HGI) en beheer (LGI) van de AHH/Datacenters (groeikern).
- Het opleiden van Defensiepersoneel.

In de voorbereiding van de aanbesteding van de *housing* en *hosting* (eerste stap) moet een besluit worden genomen of beide segmenten van de nieuwe IT-infrastructuur bij dezelfde externe partij worden belegd. De migratie van huidige omgeving naar nieuwe omgeving zal in samenwerking tussen Defensie, de partij voor AHH en overige partners worden uitgevoerd.

De volgende stappen (werkplek, netwerk (m.u.v. WAN), telecommunicatie en IT-toepassingen) zullen op een later moment in samenwerking met de markt worden gebracht conform uitgangspunten benoemd in dit document.

6. Toelichting Services

Services zijn gedefinieerd conform Rijksbrede standaard (EAR). Het onderscheid tussen IT-toepassingen en IT-infrastructuur is overeenkomstig de onderverdeling die rijksbreed gehanteerd wordt in de Enterprise Architectuur Rijk (EAR). De EAR maakt een onderscheid tussen applicatiediensten, werkplekdiensten, toegangsdiensten (beveiliging), datacenter-diensten en connectdiensten (netwerken). In dit document worden deze applicatiediensten IT-toepassingen genoemd.



Figuur 6. IT-toepassingen in relatie tot de IT-infrastructuur

In het HLO is een uitwerking gemaakt van de services binnen de IT-infrastructuur. Het HLO heeft in verband met marktconforme terminologie de Dataservices verdeelt in *Applicatiehosting* en *housing*. Hetzelfde geldt voor Netwerk services wat in het HLO meer generiek Connectiviteit wordt genoemd. Hieronder staat een korte omschrijving wat wordt verstaan onder de verschillende services (onderdelen):

- *Netwerk services (connectiviteit).* Het beschikken over verbindingen om op (LAN) en tussen locaties (WAN) te kunnen communiceren met andere gebruikers en toegang te kunnen krijgen tot IT-services. Dit kan binnen een gebouw zijn maar ook naar een operationele commandopost of de militair in het veld. Het gaat zowel om vaste verbindingen als draadloze verbindingen, inclusief satellietcommunicatie.
- *Datacenters services (applicatiehosting en housing).* De voorziening om IT-toe-passingen te kunnen hosten, gegevens te kunnen verwerken en te kunnen opslaan, zowel statisch centraal als decentraal in ontplooide situatie. Het gaat hier over de fysieke infrastructuur (datacenternetwerk, opslag, verwerking) en het applicatieplatform (besturing, gegevensbeheer, uitvoering en gegevensuitwisseling).
- *Telecommunicatie services.* De voorziening voor het bieden van spraak, tekst en beeldcommunicatie. Het gaat niet alleen om "bellen en gebeld worden" (telefoon, push-to-talk radio, e.d.) maar ook om video conferencing, semafonie, mobiele telefonie en call centers. Telefonie infrastructuren worden ook nog gebruikt voor het koppelen van faciliteiten zoals slagbomen, toegangspoortjes en liften. De spraakfunctionaliteit in het

mobiele, uitgestegen en te voet domein (MUT) is grotendeels gebaseerd op basis van diverse militaire radio's.
- *(Digitale) Werkplek services.* De voorziening voor het leveren en ondersteunen van eindgebruikersapparaten (verwerking en besturing) zoals *fat client*, *thin client*, tablet, *smart phone* en printer. Het kunnen gebruiken van generieke functionaliteiten (zoals productiviteits- , samenwerkings- en social media tools) en de toegang tot functie en bedrijfsvoeringsspecifieke functionaliteiten. Dit is de digitale werkplek.

Daarnaast zijn er twee aspecten binnen de IT-infrastructuur die betrekking hebben op bovenstaande onderdelen:

- Beheer services. Het leveren van een betrouwbare en veilige (geautomatiseerde) IT dienstverlening. Beheer betreft niet alleen het "in de lucht houden van" IT, maar ook het tijdig vernieuwen.
- Beveiligingsservice. Dit is een *enabler* om op een veilige manier digitaal te kunnen werken. Beveiliging is erop gericht om door het nemen van passende maatregelen de risico's voor de bedrijfsvoering te identificeren, te beheersen en acceptabel te houden. Beveiliging houdt ook in dat voorzien wordt in beveiligingsoplossingen (bijv. crypto, identificatiemiddelen, veilige koppelvlakken) en het implementeren van maatregelen om communicatie mogelijk te maken en te houden. Risico's zoals informatielekken, het verlies van beschikbaarheid en manipulatie van gegevens worden afgedekt.

Bijlage Definities

1. *Rubriceringsniveaus*

Rubriceringssysteem → niveau	***Hoog gerubriceerd***	***Laag gerubriceerd***
Nationale rubricering	• Stg ZEER GEHEIM • Stg GEHEIM	• Stg CONFIDENTIEEL • DEPARTEMENTAAL VERTROUWELIJK
NATO-rubricering	• COSMIC TOP SECRET • NATO SECRET	• NATO CONFIDENTIAL • NATO RESTRICTED • NATO UNCLASSIFIED
EU rubriceringen	• EU TOP SECRET • EU SECRET	• EU CONFIDENTIAL • EU RESTRICTED
Merking	•	• PERSONEELSVERTROUWELIJK • COMMERCIEEL VERTROUWELIJK • MEDISCH GEHEIM • INTERN BERAAD • INTERN GEBRUIK DEFENSIE
Politie	• Politie Zeer Geheim • Politie Geheim	• Politie Zeer Vertrouwelijk • Politie Vertrouwelijk / Politie Intern

2. *Ontplooide (deployed, mobiel en uitgestegen) omstandigheden*

Omstandigheid	Voorbeeld	Markt / Defensie
Statisch	Nederland, kazernes, vliegbases, havens.	Markt
Deployed	Compound, schip (thuishaven)	Defensie
Mobiel	In voertuig, schip (varend)	Defensie
Uitgestegen	In de contactomgeving met mogelijk geweld	Defensie