HET ROER MOET OM

DE IT VAN DEFENSIE HOOFDPIJNDOSSIER OF UNIEKE KANS?

Jacques Wetzels, Hoofddirectie Bedrijfsvoering

2014 was een gedenkwaardig jaar voor de IT van Defensie. Je zou 2014 zelfs het jaar van de IT kunnen noemen. Geen enkel ander defensiedossier trok in korte tijd zoveel aandacht van de media als de IT. Enkele ernstige verstoringen in korte tijd zorgden daarvoor. Gevolg was dat IT ook hoog op de politieke agenda kwam en de minister besloot tot diepgaand onderzoek. Met het verschijnen van enkele kritische rapporten werd duidelijk dat het roer om moest. Dit was de opmaat voor grote veranderingen in de IT van Defensie en voor de mensen die daarbij betrokken zijn. Defensie heeft daarna zeker niet stilgezeten en er zijn ondertussen grote stappen gezet. Waar staat Defensie nu en wat kunnen we de komende jaren verwachten? →

Inleiding

IT en overheid hebben al jaren een moeizame relatie. De commissie Elias sprak in niet mis te verstane bewoording over de alarmerende situatie rond grote IT-projecten bij de overheid.
Ook Defensie kan al jaren rekenen op warme belangstelling van de pers als het gaat over het grootste IT-programma van Defensie, namelijk de invoering van ERP voor materieellogistiek en financiën. Dit IT-programma is bekend onder de naam SPEER. Het is daarom niet verwonderlijk dat enkele ernstige verstoringen in de IT van Defensie de volle aandacht kregen van pers en politiek. Was de IT van Defensie nog wel op orde en toereikend voor missies? Hoe had het zover kunnen komen? En de belangrijkste vraag: “Hoe nu verder?”

De minister liet extern onderzoek instellen en daaruit kwam naar voren dat de belangrijkste knelpunten voor de recente verstoringen in de techniek lagen, met name in de infrastructuur en de rekencentra. Er waren kwetsbaarheden geconstateerd die aangepakt moesten worden om de continuïteit voor Defensie te waarborgen. Met name veroudering van apparatuur deed het risico op uitval toenemen terwijl tegelijkertijd onvoldoende reservecapaciteit beschikbaar was om uitval op te vangen. De minister informeerde de Tweede Kamer hierover op 1 juli 2014 middels een brief.

De continuïteit van de missies werd niet direct geraakt door deze problemen omdat de ontstane situatie vooralsnog alleen de systemen raakte voor de kantoorautomatisering. De meest acute knelpunten konden bovendien snel worden verholpen, in ieder geval voor de korte termijn. Nu was de vraag: hoe had dit ooit zover kunnen komen in een ministerie waarvoor IT zo belangrijk is? De permanente bezuinigingen op Defensie hadden ook bij de IT van Defensie hun tol geëist. De grote reorganisatiegolf ten gevolge van de beleidsbrief 2011 had geleid tot vertrek van personeel en de aandacht was primair op reorganiseren gericht in plaats van investeren.

De belangrijkste conclusies van de onderzoeken waren:

- Verouderde apparatuur en achterstand met moderniseren;
  - Vooral hardware was technisch verouderd en had in een aantal gevallen al vervangen moeten zijn door nieuwere en modernere varianten. Dat was om redenen van kostenbesparing niet gebeurd.
- Onvoldoende reservecapaciteit om uitval op te vangen;
  - Capaciteit binnen de rekencentra was onvoldoende om taken van andere rekencentra over te nemen bij verstoringen.
- De besturing van IT was onvoldoende effectief en het ontbrak aan een heldere visie bij de top;
  - Er was al jarenlang op kosten gestuurd en fors bezuinigd zonder echt een strategie te hebben wat Defensie op langere termijn met IT wil.
- De samenwerking tussen belangrijke spelers in de IT-keten was niet optimaal;
  - De IT-keten was verdeeld over verschillende partijen. Er was echter onvoldoende samenwerking en de processen van de verschillende partijen waren niet op elkaar afgestemd.

Wat gebeurde er daarna?

De ontstane situatie leek op het eerste gezicht alleen negatieve kanten te kennen. Er moest heel veel gebeuren om de IT weer helemaal op orde te krijgen. Maar er was ook een keerzijde met positieve effecten. De beeldvorming over IT bij het topbestuur van Defensie was fundamenteel veranderd. Het topbestuur besefte dat IT geen bijzaak is maar een belangrijke *enabler* voor de business die voortdurend managementaandacht moet krijgen vanuit de top van de organisatie. Het belang van IT stond niet langer ter discussie en ook de gevolgen waren duidelijk geworden als er niet vanuit een toekomstvisie sturing wordt gegeven aan zo’n belangrijk domein. Het was voor de top van de organisatie duidelijk geworden dat IT

op toegevoegde waarde moet worden bestuurd en niet alleen op kosten. De gevolgen van het besturen van IT als kostenpost waren evident en de zeer beperkte aandacht die IT had gehad vanuit het topbestuur paste niet langer bij een organisatie die zo verweven is met IT. Er ontstond een breed gedragen beeld bij het topbestuur dat de rol van IT steeds belangrijker wordt in een wereld die zich kenmerkt door razendsnelle technologische ontwikkelingen. Er is vrijwel geen wapensysteem meer dat niet uitgerust is met complexe IT, het speelveld van inlichtingen speelt zich grotendeels af in de digitale wereld en tegenstanders in inzetgebieden weten zich flexibel en slagvaardig te organiseren met eenvoudig verkrijgbare communicatiemiddelen. Voor terroristische organisaties heeft het internet met sociale media inmiddels de rol van een effectief commandovoeringsysteem ingevuld. Met verouderde IT zou Defensie op termijn de concurrentie met deze ontwikkelingen niet aan kunnen, met alle risico´s van dien.

De Bestuursraad (het hoogste ambtelijke bestuursorgaan binnen Defensie onder leiding van de SG), heeft inmiddels maatregelen genomen om de zorgelijke situatie in de IT aan te pakken. Daarbij is niet alleen gekozen voor het repareren van de ontstane kwetsbaarheden, maar voor het ontwikkelen van een nieuwe visie op IT, die recht doet aan de waarde van IT voor Defensie en past bij de snel veranderende wereld. Een eerste belangrijke stap op het gebied van visie is gezet in oktober 2014 met de visie op IT, onder de naam: *'Let's make IT happen!'* Deze visie schetst een beeld van de toekomstige omgeving waarin Defensie moet kunnen opereren en leidt daarvan af aan welke eisen de IT in de toekomst moet voldoen. De visie definieert drie pijlers, namelijk continuïteit, beveiliging en innovatie. Deze visie op IT schetst de belangrijkste trends en ontwikkelingen waarop Defensie met behulp van IT zal moeten inspelen. De visie onderstreept dat IT van strategische waarde is, tijdens alle fasen van militaire gereedstelling en inzet en dat de IT van Defensie wendbaar en flexibel moet zijn. Naast de visie is er gekozen voor een breed pakket aan maatregelen om de eerder genoemde knelpunten aan te pakken, zoals deze ook zijn verwoord in de brief van de minister aan de Tweede Kamer van 1 juli 2014. Deze maatregelen zijn deels organisatorisch van aard en deels gericht op het wegnemen van technische kwetsbaarheden.
Daarnaast is de weg ingeslagen die is gericht op een flexibele en innovatieve IT voor de toekomst en de besturing vanuit de top die daarbij hoort. De kans op succes zit immers niet alleen in de techniek, ook de organisatie en vooral het topbestuur moet IT weer als een eigen verantwoordelijkheid gaan zien.

Een mix van maatregelen

Er is dus gekozen voor een mix van maatregelen. De eerste stap was het betrekken van topbestuurders bij IT.
Er is een *IT Governance Board* (ITGB) ingesteld en de positie van de *Chief Information Officer* (CIO) is versterkt. Er is een assessment uitgevoerd om kwetsbaarheden in de IT te inventariseren. De technische kwetsbaarheden worden weggenomen in de bestaande IT-infrastructuur. Tegelijkertijd wordt gewerkt aan een nieuwe IT-infrastructuur die de basis vormt voor de innovatieve IT van de toekomst.

Er komt dus nieuwe IT, in eerste instantie naast de huidige IT. Deze nieuwe IT zal de huidige IT geleidelijk vervangen. Voor deze aanpak is heel bewust gekozen omdat de huidige IT veel te complex is om in één keer te vervangen en bovendien heeft de huidige IT nog delen die nog jaren in gebruik kunnen blijven. Wat de nieuwe IT vooral kenmerkt is de stand der techniek die daarvoor gebruikt gaat worden. De nieuwe IT is innovatief, sluit veel meer aan bij de wereldwijde ontwikkelingen, zoals cloudoplossingen, mobiel werken en is toegerust op de enorme toename van data.

Defensie gaat deze nieuwe IT-infrastructuur niet meer helemaal zelf ontwikkelen en beheren. Intensief samenwerken met de markt is het credo. In sommige delen van de nieuwe IT-infrastructuur speelt de markt een grote rol in het beheer, in ieder geval in de laag-gerubriceerde delen en binnen Nederland. Delen van de IT-infrastructuur die ontplooid worden toegepast en delen die hoog-gerubriceerd zijn, zullen grotendeels door Defensie zelf worden beheerd. Ontwikkeling zal vrijwel altijd samen met de markt plaatsvinden. Zo ontstaat een situatie waarbij Defensie zelf in stand kan houden wat nodig is voor de kerntaken en kan kennis en kunde van marktpartijen optimaal worden benut. De regie over het geheel ligt bij Defensie zelf.
De nieuwe IT-infrastructuur wordt ook niet in een keer neergezet (geen *big bang*). Er wordt gestart met een zogenaamde groeikern. Dat is een eerst oplevering van de nieuwe IT-infrastructuur met een beperkte capaciteit, maar wel hypermodern. Vanuit deze groeikern wordt gestaag verder gebouwd in kleine behapbare projecten.

Op dit moment (februari 2016) bereidt DMO de aanbesteding van de nieuwe IT-infrastructuur voor.

"Wat de nieuwe IT vooral kenmerkt is de stand der techniek die daarvoor gebruikt gaat worden."

Business eisen

De toekomstige rol van IT is het optimaal ondersteunen van de beoogde businesseisen zoals deze in november 2014 zijn geïnventariseerd door CDS en HDBV, namelijk:

- Business en 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 voor zeer grote hoeveelheden informatie.
- De IT is eenvoudig en snel aanpasbaar.

De belangrijkste maatregelen op een rijtje

De ITGB

Er is een *IT Governance Board* (ITGB) ingesteld die fungeert als voorportaal voor de Bestuursraad op het gebied van de IT. De ITGB brengt onderwerpen ter besluitvorming in bij de Bestuursraad. De kern van de ITGB wordt gevormd door de *demand*-organisatie (behoeftesteller, directeur Plannen van de CDS), de *supply*-organisatie (leverancier, de directie van DMO/JIVC en OPS) en de CIO (de Hoofddirecteur Bedrijfsvoering), aangevuld met een directeur van de Hoofddirectie Financiën en Control, een vertegenwoordiger van de Hoofddirecteur Beleid en de plaatsvervangend commandanten van de defensieonderdelen. In de ITGB wordt besluitvorming voorbereid over IT-vraagstukken. De Bestuursraad wordt hiermee ondersteund in de besluitvorming over IT.

De ITGB is een belangrijke stap om voor IT-vraagstukken de brug te slaan tussen het hoogste bestuurlijke niveau en de bij IT betrokken organisatiedelen. Tevens vormt de ITGB een platform om de communicatielijnen over IT kort te houden en de afstemming tussen demand, supply, CIO en de lijncommandanten te faciliteren. De ITGB vergadert maandelijks, vaker indien de situatie dat vereist.

De positie van de CIO

De positie van de CIO is versterkt door deze op te nemen in de Bestuursraad. De CIO-rol is belegd bij de Hoofddirecteur Bedrijfsvoering (HDBV). Deze had voorheen uitsluitend een adviserende rol. Sinds de toetreding van de CIO tot de Bestuursraad en het instellen van de ITGB heeft de CIO veel meer een sturende rol over de toekomstige koers van de IT die in nauwe samenwerking met de CDS wordt ingevuld. Daarmee wordt geborgd dat IT de focus houdt op het primaire proces van Defensie.

De CIO wordt ondersteund door een CIO Office waarin een aantal IT-deskundigen de CIO adviseren. Vanuit de CIO Office worden ook de contacten met andere departementen onderhouden om rijksbrede initiatieven op elkaar af te stemmen. Tevens beheert de CIO Office de zogenaamde Enterprise Architectuur, oftewel de koers van de IT voor de lange termijn, afgestemd op de ontwikkelingen van de bedrijfsvoering van Defensie. Tot slot heeft het CIO-Office een toetsende rol, voorafgaand aan de start van IT-projecten (CIO-oordeel).

Managementwissel

Het nieuwe management bij JIVC en Operations is aan het werk gegaan met nieuw elan, frisse inzichten en een ruime ervaring die deels van binnen en deels van buiten Defensie komt. Dat komt de samenwerking tussen de verschillende geledingen inmiddels merkbaar ten goede. JIVC en Operations werken steeds meer alsof het één bedrijf is.

IT-assessment

Om alle tekortkomingen van de bestaande IT op te sporen heeft een zogenaamd IT-assessment plaatsgevonden. Daarbij is beoordeeld wat de technische staat is van alle cruciale elementen van de huidige IT.
Dat heeft geleid tot een integraal beeld op welke punten de IT op orde is en op welke punten actie noodzakelijk is. Dit assessment is een verdieping geweest op basis van het eerste onderzoek waarover de minister in juli 2014 de Kamer heeft geïnformeerd. Dit assessment heeft ook inzicht gegeven welke delen van de IT nog prima op orde zijn en dus niet gelijk hoeven te worden vervangen door nieuwe IT.

High Level IT ontwerp (HLO)

Nieuwe IT begint met een ontwerp. Maar wat moet je ontwerpen als je niet weet waaraan de IT van de toekomst moet voldoen? Om zeker te weten dat de nieuwe IT aansluit bij de behoeften van de onderdelen is in oktober en november 2014 door CDS en HDBV een inventarisatie uitgevoerd van de business-eisen. Dit zijn de eisen waaraan nieuwe IT zou moeten voldoen vanuit de optiek van de Defensieonderdelen en de MIVD. Dit is gebeurd door commandanten of diens plaatsvervangers persoonlijk te interviewen over hun visie op de toekomst van Defensie, en de rol die IT daarin zou moeten vervullen. Daarbij is gesproken over veranderingen binnen Defensie, maar ook over trends in de maatschappij, technologie en politiek, nieuwe vormen van samenwerking en de gevolgen voor de primaire taken.

De interviews hebben een schat aan informatie opgeleverd over de rol die IT in de toekomst moet vervullen. Uit de gesprekken is duidelijk naar voren gekomen dat, wil Defensie klaar zijn voor de toekomst, de rol van IT duidelijk anders moet zijn dan nu. Er zal veel meer gestuurd moeten worden op de effecten die beoogd zijn en de rol die IT daarin vervult. Niet de systemen moeten centraal staan, maar de mensen en hun taken en ten slotte moet de IT zich zeer snel kunnen aanpassen. Veel systemen waar medewerkers nu mee werken zijn opgebouwd vanuit voorspelbare processen (procesgestuurde IT). Medewerkers hebben steeds meer behoefte aan IT met flexibele processen om een taak uit te voeren en samen te werken (*case* gestuurde IT). Dat houdt in dat processen niet altijd op dezelfde manier verlopen en de medewerkers meer keuzevrijheid hebben. Zulke moderne systemen zijn dus vooral beslissingsondersteunend en laten ruimte voor eigen keuzes.

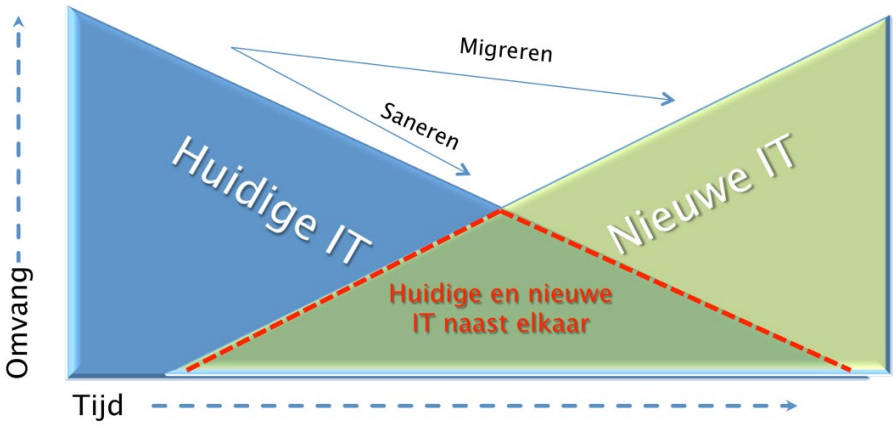
Op basis van deze inzichten is een ontwerp gemaakt, het *High Level* IT-ontwerp (HLO). Dit ontwerp bevat nog geen bouwtekening maar formuleert keuzes en richtlijnen voor de nieuwe IT. Een voorbeeld van zo'n richtlijn is dat de nieuwe IT uit losse modules moet bestaan die snel vervangen kunnen worden. Het HLO kan worden vergeleken met het bestemmingsplan van een gemeente waarin op hoofdlijnen staat wat de spelregels en keuzes zijn om te ontwikkelen per deelgebied van de IT, zoals de technische infrastructuur, de applicaties, de beveiliging etc. Het HLO is de eerste stap in het vertalen van de visie naar de realisatie. Dit ontwerp was in april 2015 helemaal gereed.

Het beeld dat de interne of externe leverancier van IT zelf wel bedenkt wat goed is voor de gebruiker is hiermee definitief verlaten. De kennis vanuit de defensieonderdelen en de MIVD is voortdurend de leidraad geweest om de het HLO uit te werken.

Wat bedoelen we eigenlijk met rationalisatie?

In relatie tot de nieuwe IT wordt ook vaak het begrip rationalisatie genoemd. Daarmee wordt bedoeld dat de huidige 2500 verschillende IT-toepassingen zo snel mogelijk worden verminderd. Er is inmiddels een traject gestart om de toepassingen te categoriseren naar domein, bijvoorbeeld logistiek, en vervolgens wordt bepaald wat de toekomst voor de toepassing moet zijn. Daarbij wordt gekeken of de toepassing moet blijven bestaan of op termijn kan verdwijnen. Uiteraard wordt er niets uitgezet voordat dit met de gebruikers is afgestemd.

Het HLO bevat verschillende onderdelen. Het eerste deel gaat over de informatie die bij de commandanten is verzameld en een vertaling naar business eisen en gewenste business effecten, en de rol die IT daarin zou moeten vervullen. Het tweede deel gaat over de richting waarin het complexe systeemlandschap van Defensie zich moet ontwikkelen, rekening houdend met het feit dat Defensie momenteel circa 2500 verschillende toepassingen gebruikt. Het derde deel gaat over de modernisering van de techniek, zoals netwerken, rekencentra, werkplekken etc. Het vierde deel ten slotte gaat over de veranderstappen. Voor de partijen die de nieuwe IT gaan realiseren is het HLO heel belangrijk. Het HLO bevat alle spelregels



De huidige staat van de IT sluit niet aan bij het ambitieniveau van onze krijgsmacht. Hieraan liggen de volgende oorzaken aan ten grondslag:

- De technische IT-infrastructuur bevat kwetsbaarheden en is verouderd.
- De gemoderniseerde IT (zowel de infrastructuur als de toepassingen) moet flexibel en snel veranderbaar zijn. Een modulaire opbouw is daarvoor essentieel.
- Om informatiedominantie te behouden moet Defensie in staat zijn voortdurend te innoveren en te experimenteren. De gemoderniseerde IT moet de basis leggen voor een innovatie- en beproevingsdomein waarmee Defensie continu nieuwe ontwikkelingen kan volgen.
- Voor de gemoderniseerde IT moet drastisch gesaneerd worden in het aantal toepassingen.
  Voor de resterende toepassingen moeten voorzieningen voorhanden zijn waarmee deze voor de gebruikers als één logisch geheel gaan werken en aansluiten bij taak, rol of functie.

waaraan de realisatietrajecten moeten voldoen. Als je het vergelijkt met de analogie van de stedenbouw dan is het HLO het bestemmingsplan dat bepaalt wat een projectontwikkelaar op een bepaalde locatie kan en mag bouwen en welke spelregels er gelden.

Waarom oude en nieuwe IT naast elkaar?

Een belangrijk keuzemoment voor de schrijvers van het HLO was het vernieuwen van de bestaande IT of helemaal opnieuw beginnen. Beide opties hebben voordelen en nadelen. Uiteindelijk is toch de keuze gemaakt om de bestaande IT niet meer te gaan vernieuwen maar een nieuwe start te maken met moderne IT, naast de oude IT.
Deze keuze is gemaakt omdat verschillende onderzoeken (intern en extern) consistent waren over de staat van de huidige IT. De huidige IT is verouderd, complex (vele koppelingen), een bonte verzameling van oplossingen en slechts met grote moeite te moderniseren. Dat zou betekenen dat de huidige IT tegen grote kosten en inspanning geleidelijk vernieuwd zou moeten worden, maar de complexiteit zou daarbij grotendeels blijven bestaan, door de enorme diversiteit van oplossingen.

Daarnaast zou vernieuwen van de bestaande IT het streven naar intensieve samenwerking met de markt en daarmee naar een meer innovatieve IT, enorm in de weg staan. De keuze is nu gemaakt om de huidige IT niet meer te moderniseren maar deze wel netjes in stand te houden, zolang als nodig.

Daarnaast wordt nieuwe IT ontwikkeld, op basis van de keuzes die in het HLO zijn uitgewerkt. Dat betekent dat de nieuwe IT wordt gebouwd met de modernste technieken, optimaal afgestemd op internettechnologie en in lijn met de toekomstverwachtingen. Deze nieuwe IT wordt modulair opgebouwd, is snel veranderbaar, wereldwijd toegankelijk en is in Nederland niet wezenlijk anders dan in het inzetgebied.
Wat nog bruikbaar is in de huidige IT wordt gemigreerd (verhuisd) naar de nieuwe IT en wat niet meer bruikbaar is wordt geleidelijk gesaneerd (rationaliseren).

In onderstaand overzicht is dit vereenvoudigd weergegeven.

Verantwoordelijkheid voor	Ontwikkelen & Realiseren	Beheren	Integreren (regie)
Hoog Gerubriceerde Infrastructuur	Markt/Defensie*	Defensie	Defensie
Laag Gerubriceerde Infrastructuur – statisch	Markt	Markt	Defensie
Laag Gerubriceerde Infrastructuur – ontplooid	Markt	Defensie	Defensie

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

Binnen de verantwoordelijkheidsverdeling worden activiteiten door de partners en Defensie gezamenlijk uitgevoerd binnen de regels en kaders van de verantwoordelijke.

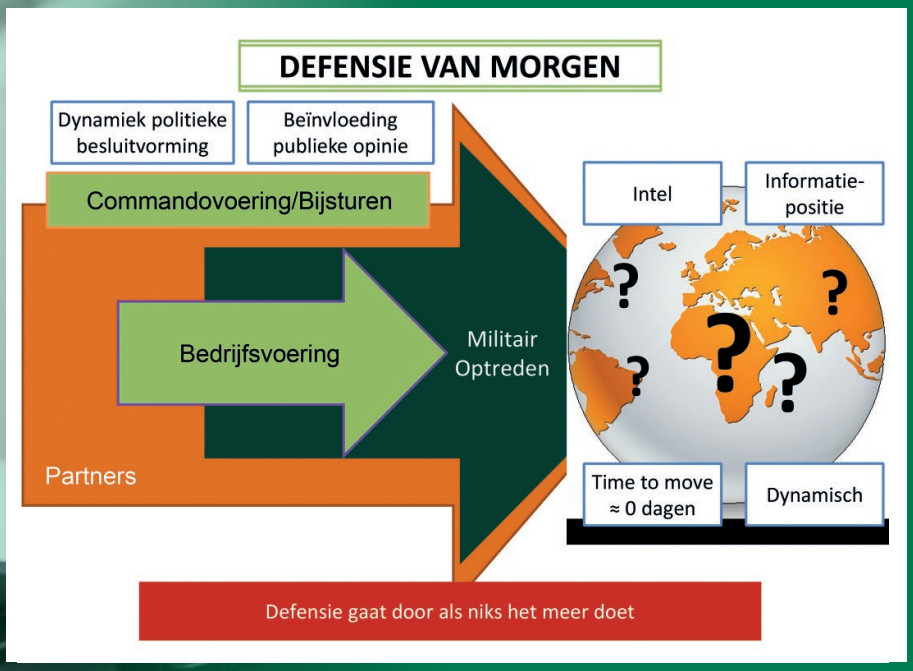
Do-IT en GrIT

Het uitwerken van een IT-visie en het HLO mag met recht een prestatie wor-

den genoemd. In relatief korte tijd heeft Defensie een duidelijke koers uitgezet en het 'bestemmingsplan' voor de IT bepaald. Maar daarmee was het niet af. Voor DMO begon het werk toen pas echt. Op basis van het HLO is DMO (JIVC en OPS) begonnen met het verdiepen en concretiseren van het HLO (zie de DMO als de projectontwikkelaar in de stad die op basis van het bestemmingsplan de projectplannen gaat ontwikkelen). Dat is gedaan met een enorme personele inspanning. Op sommige momenten waren meer dan 60 medewerkers van DMO bezig met het analyseren van het HLO en het uitwerken van alle consequenties om nieuwe IT daadwerkelijk te ontwikkelen. Dit was nodig omdat een belangrijk deel van de realisatie van de nieuwe IT met marktpartijen gebeurt.

Een marktpartij kan alleen oplossingen leveren als duidelijk omschreven is wat Defensie van de oplossing verwacht. Het HLO was daarvoor nog niet concreet genoeg. Het traject binnen DMO om deze vertaalslag en verdiepingsslag te maken is in een tijdelijk project gedaan bekend onder de werknaam Defensie Ontwerp IT, oftewel Do-IT. Resultaat is een aantal documenten die houvast bieden voor partijen die daadwerkelijk gaan bouwen (de projectontwikkelaar heeft de analyses klaar waarmee de architect en aannemer weer verder kunnen).

Ondertussen is een programma gestart binnen DMO dat de aanbesteding gaat doen voor de nieuwe IT. De naam van dat programma is Grensverleggende IT, oftewel GrIT. De resultaten van Do-IT zijn overgedragen aan het programma GrIT. Dit programma is op dit moment op stoom om zo snel mogelijk een marktpartij te kiezen voor de realisatie van het eerste deel van de nieuwe IT, oftewel de zogenaamde groeikern.



Samenwerken met de markt

Samenwerken met de markt is een essentieel onderdeel van de nieuwe IT maar dat lukt alleen wanneer er een duidelijke verantwoordelijkheidsverdeling is. Wanneer die ontbreekt of onduidelijk is dan zal de opdrachtgever vrijwel altijd zelf de volledige verantwoordelijkheid dragen. Daarom is bij de verantwoordelijkheidsverdeling gekozen voor een taakverdeling die neerkomt op het volgende:

- Voor de statische, laag-gerubriceerde infrastructuur zal Defensie zoveel mogelijk van de verantwoordelijkheden beleggen bij de markt, met uitzondering van de verantwoordelijkheid voor het integreren.
- Zodra laag-gerubriceerde infrastructuur echter ontplooid wordt gebruikt, dan zal Defensie ook de verantwoordelijkheid voor het beheer zelf houden.
- Voor de hoog-gerubriceerde infrastructuur draagt Defensie in principe zelf de verantwoordelijkheid.

Trendbreuk

De situatie op het gebied van IT binnen Defensie kan worden gezien als een trendbreuk ten opzichte van het verleden. Er moet nog veel gebeuren, maar er is op een aantal cruciale punten een enorme stap gezet.
De wijze waarop de commandanten zijn betrokken bij de visievorming is duidelijk anders dan in het verleden. Hun kennis is voortdurend meegewogen in de ontwerpbeslissingen.

De organisatorische maatregelen, zoals het instellen van de ITGB en de positionering van de CIO, waarborgen de betrokkenheid van het topbestuur. Innovatie en veranderbaarheid van IT komen centraal te staan. Dat zal gevolgen hebben voor de manier waarop met projecten wordt omgegaan.

Het credo 'sturen op effect' heeft eveneens grote gevolgen. IT zal niet langer een kostenpost zijn, maar een middel om gewenste doelen en beoogde effecten van Defensie mogelijk te maken.

De uitdaging voor Defensie zal de komende jaren zijn om de oude IT in beheersbare stappen af te bouwen en nieuwe, innovatieve IT, te ontwikkelen. Samenwerking met de markt is daarvoor cruciaal.