Ministerie van Defensie

Visie op IT:

let's make IT happen!

Visie op IT:
let's make IT happen!

Versie 2.1.0 - Oktober 2014

Inhoud

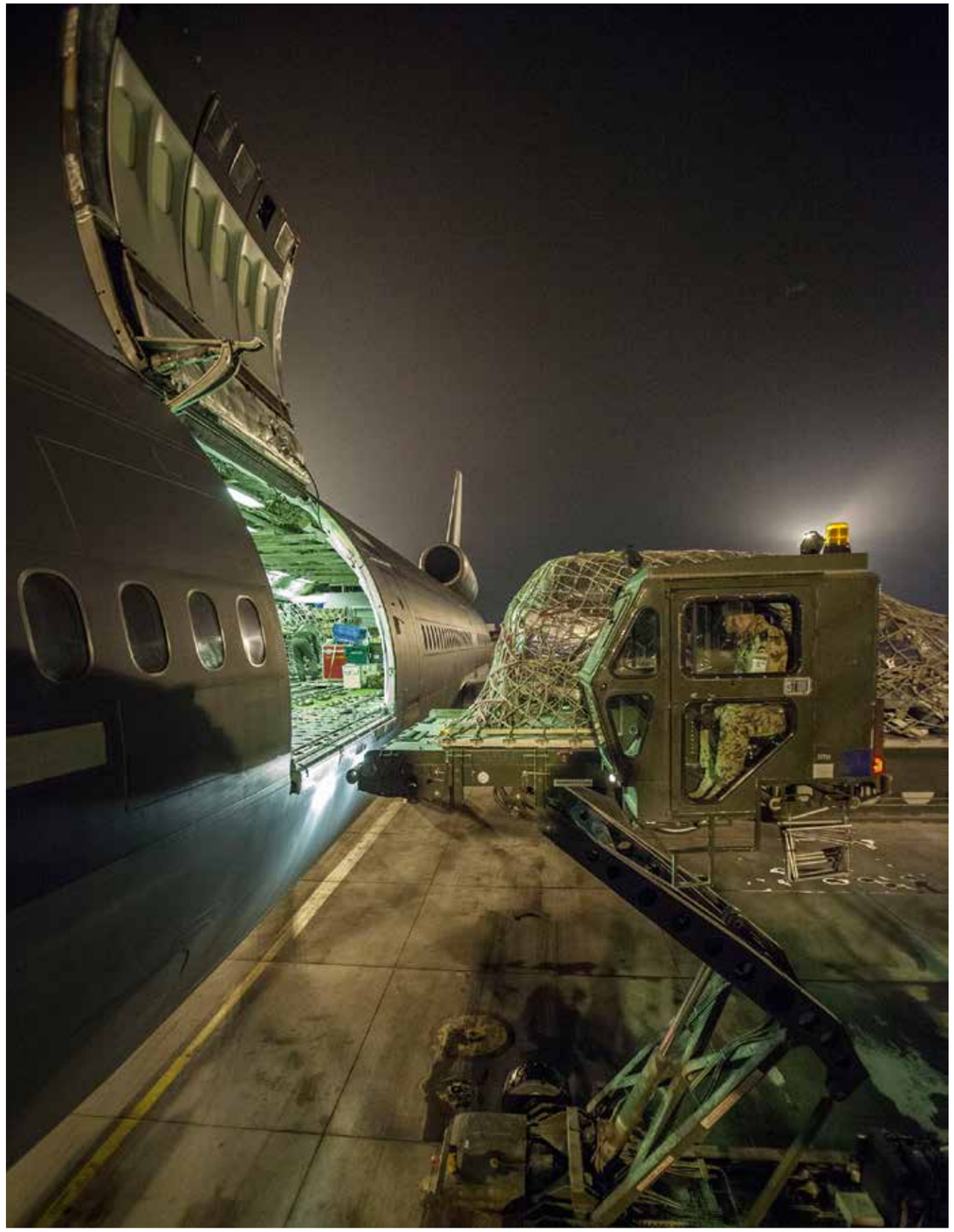
1. Inleiding

Voor u ligt de visie van Defensie op Informatietechnologie (IT)[1] als integraal en onverbrekelijk onderdeel van de operationele processen, de bedrijfsvoering en de inlichtingenketen. Waarom is deze visie opgesteld? Omdat IT voor de krijgsmacht een strategische *enabler* is die zich in een razend tempo (door-)ontwikkelt. Het is een *game changer* die een ongekende én richtinggevende invloed heeft op zowel bedrijfsvoering als operaties.

Uit de praktijk blijkt dat toekomstvoorspellingen een beperkte houdbaarheid hebben. Wat vandaag de dag als onmogelijk wordt gehouden, kan binnen enkele jaren en soms enkele maanden *common technology* zijn. Denk bijvoorbeeld aan de *smart phone*, de *tablet* en mobiele data. Tegelijk kunnen verouderde technologieën soms een langere levensduur hebben dan eerder werd voorspeld. Een voorbeeld is koperdraad als primair transportmiddel. Eén ding is zeker: de toekomst zal niet zo zijn zoals we hadden verwacht.

Dit document is dan ook niet opgesteld om exact te formuleren hoe de IT van Defensie er over pakweg tien jaar uitziet. Wel is op basis van de drie pijlers “continuïteit, beveiliging en innovatie” een visie geformuleerd waar de organisatie in functionele zin behoefte aan heeft. Doel is om te profiteren van relevante nieuwe mogelijkheden (innovatie) om blijvend en op een veilige wijze (beveiliging) haar slagkracht te garanderen (continuïteit). Als vervolg op deze visie wordt een stappenplan opgesteld. Dit plan beschrijft de weg voor de daadwerkelijke invulling van de visie. Aan de hand van actuele ontwikkelingen zal deze weg worden bewandeld en naar behoefte worden aangepast.

[1] Informatietechnologie (IT) is de technologie die als hulpmiddel dient om de techniek van het verzamelen, vastleggen, verwerken, bewerken, bewaren, representeren en transporteren van gegevens uit te voeren.



2. Op weg naar een flexibele bedrijfsvoering

2.1 Rol IT in de krijgsmacht

De Nederlandse krijgsmacht moet voorbereid blijven op een scala aan inzetmogelijkheden, in alle fasen van een conflict en indien nodig op grote afstand van Nederland [2]. De informatiemaatschappij speelt hierbij een belangrijke rol. Rivaliserende partijen maken bijvoorbeeld veelvuldig gebruik van steeds goedkopere, flexibelere en krachtigere middelen voor communicatie en informatieuitwisseling. De maatschappij wordt sowieso gedreven door IT. Vele ontwikkelingen hebben, dan wel krijgen, invloed op ons leven zoals de doorontwikkeling van *smart phones*, *internet-of-things*, *Google Glass*, *3D-printing*, *cloud*, *video everywhere*, sensor-technologie, big data en 4G/5G. Alleen organisaties die deze nieuwe technologieën weten te benutten kunnen zich onderscheiden ten opzichte van anderen. Alleen al vanuit deze invalshoek kan IT voor organisaties geen kostenpost meer zijn, maar een voorwaarde om datgene waar ze voor staan effectief en efficiënt te kunnen uitvoeren.

Het is niet te voorspellen hoe IT zich de komende jaren verder ontwikkelt en wat dat exact voor de krijgs-macht betekent. Helder is wel dat IT een onlosmakelijk onderdeel van onze bedrijfsvoering is en zal zijn: het zit in de haarvaten van de organisatie. De krijgsmacht kan haar taken alleen effectief en doelmatig uitvoeren als ze beschikt over operationele capaciteiten met een adequaat functionerende bedrijfsvoering ondersteund door moderne en goed werkende (toereikende, beheersbare, flexibele en betaalbare) IT.

De wendbaarheid *(agility)* van de krijgsmacht en haar processen bepaalt in welke mate zij in staat zal zijn gebruik te maken van de razendsnelle ontwikkelingen in de IT. Oftewel, hoe snel en flexibel kan de krijgsmacht inspelen op veranderingen en mee bewegen met de nieuwe ontwikkelingen en technologie? De krijgsmacht moet nieuwe manieren vinden om innovatief te zijn zonder de continuïteit van de bedrijfs-voering en de beveiliging van haar systemen en data in gevaar te brengen. Dit vereist ook flexibiliteit en adaptief vermogen in de bedrijfsvoering.

De volgende ontwikkelingen onderstrepen het belang van deze zorgvuldige balans:

1. ***Wapensystemen in het digitale tijdperk.*** Wapensystemen bevatten steeds meer IT. Bijvoorbeeld het F-35 gevechtsvliegtuig. De missiecomputer koppelt alle sensoren (zoals CCTV, IR en radar) aan elkaar om een gecombineerde inschatting te maken van de dreiging. Hierdoor is de piloot op de hoogte van de actuele "360 graden dreiging" en weet hij/zij bovendien of de vijand hem/haar "kan zien". Dit systeem is uniek. Het systeem presenteert dit niet alleen aan de piloot, maar ook aan alle anderen (zowel in de lucht, op de grond als op zee) die gebruik moeten maken van deze informatie. Dit geïntegreerd optreden met behulp van *Network Enabled Capabilities* (NEC) staat voor het effectief gebruiken van informatie. Ofwel, een samenhangend geheel van militair operationele processen dat wordt ondersteund door moderne netwerk- en communicatietechnologieën. Dit brengt met zich mee dat grote hoeveelheden gegevens worden verzameld en verwerkt voor commandovoering, inlichtingenvergaring en wapeninzet. Zonder toereikende IT kan dat niet effectief plaatsvinden. IT kan ook ingezet worden als hoofdwapensysteem, zoals offensief optreden in het cyberdomein.

2. ***Informatiegestuurd Optreden.*** De Commandant der Strijdkrachten (CDS) hanteert Informatiegestuurd Optreden (IGO) als belangrijk uitgangspunt in het speerpunt "Vernieuwing Operationeel Domein". De focus ligt op informatiedominantie en een ononderbroken, en volledig gedeelde en gepersonaliseerde *Situational Awareness* (SA) en *Situational Understanding* (SU). Het huidige en toekomstige optreden van Defensie vereist dat essentiële functionaliteiten van informatievoorziening en commandovoering flexibel, schaalbaar, adaptief en integraal over de hele keten van sensor naar effector kunnen worden uitgevoerd. Operaties in grote operatiegebieden met beperkte middelen dwingen tot gerichte effectieve inzet van militair vermogen. IGO vloeit voort uit het genetwerkt samenwerken en wordt gekenmerkt door adequate middelen, afgestemde procedures, een integraal netwerk van deelnemende eenheden en

[2] Nota "In het belang van Nederland", oktober 2013.

organisaties en van gevalideerde informatie en inlichtingen. IGO stelt de organisatie in staat om in de toekomst doelgericht haar capaciteiten in te zetten en haar taken, operationeel effectief, uit te voeren.

3. ***Geïntegreerde bedrijfsvoering.*** Defensie werkt aan geïntegreerde bedrijfsprocessen. De invoering van *Enterprise Resource Planning* (ERP) is hiervan een voorbeeld. Hiermee kan de operationele *footprint* worden verkleind. Dit stelt hoge eisen aan de betrouwbaarheid van IT. Ook in de juridische, personele en medische processen is IT onmisbaar. Voorts maken eenheden in het operationele domein ook steeds meer gebruik van dit soort systemen. Daarmee vervaagt het onderscheid tussen IT voor de operationele taakuitvoering en voor de bedrijfsvoering. Vanuit de (operationele) behoefte moet dan ook heel bewust worden gekozen voor een beschikbaarheidsniveau van dit soort systemen.

4. ***Samenwerking.*** Defensie kiest voor samenwerking met strategische partners en marktpartijen (zoals NATO, interdepartementaal, veiligheidsketen, *multi-agency* of leveranciers) om capaciteiten te *sharen* dan wel te *poolen*. Bij iedere vorm van samenwerking hoort het uitwisselen van informatie. Zonder adequate IT is dit niet meer mogelijk. Uit bijvoorbeeld de intensieve samenwerking met België (BENESAM) blijkt dat koppelingen tussen netwerken en toegang tot elkaars systemen steeds gangbaarder worden. Ook met internationale leveranciers van wapensystemen zijn beveiligde IT-verbindingen onmisbaar geworden in elke fase van ontwerp, ontwikkeling, productie, levering en gebruik.

5. ***Cyber defence en veiligheid.*** De technologische ontwikkelingen in de samenleving hebben grote invloed op onze veiligheid. Bedreigingen van buiten nemen toe. Ontwikkelingen zoals cyberaanvallen, virussen en *malware* leiden tot een wedloop tussen indringers en beveiligingsmaatregelen. De afhankelijkheid van digitale middelen leidt ook voor de krijgsmacht tot kwetsbaarheden die urgente aandacht behoeven. En het spreekt voor zich dat de impact op de samenleving van een grootschalige cyberaanval enorm kan zijn. De krijgsmacht wil ook in het digitale domein haar rol als “zwaardmacht” naar behoren vervullen. Het voortdurend bewaken, monitoren en innoveren in IT is dan cruciaal.

2.2 De pijlers onder het fundament van de IT

Het belang en invloed van IT op zowel de bedrijfsvoering als de operationele inzet is groot. Het is een onmiskenbare *enabler* voor de gehele organisatie. Het fundament onder de doorontwikkeling van IT als integrale *enabler* rust op de volgende drie pijlers:

1. ***Continuïteit.*** De betrouwbaarheid van de IT is van wezenlijk belang. Zonder goed functionerende en betrouwbare IT geen inlichtingen, geen missies, geen bedrijfsvoering en dus geen goed functionerende krijgsmacht. Voor de inrichting van de continuïteit is een zorgvuldig vastgesteld risicoprofiel een vereiste.

2. ***Beveiliging.*** De aard van de krijgsmacht stelt hoge eisen aan de beveiliging. De beveiliging van IT-systemen en de integriteit van data moeten dan ook gegarandeerd zijn.

3. ***Innovatie.*** Met de ambitie om goed voorbereid te blijven op een scala aan inzetmogelijkheden is het noodzakelijk om slim gebruik te maken van nieuwe mogelijkheden. De krijgsmacht moet een wendbare (agile) organisatie zijn en blijven om “anderen” een stap voor te zijn.

Binnen de krijgsmacht kent IT verschillende toepassingsgebieden: IT als hoofdwapensysteem (zoals *cyber*), IT als onderdeel van een wapensysteem en IT als ondersteuning van de processen in de organisatie. In de eerste twee domeinen gaat het veelal om specifieke IT (de zogenoemde strategische IT) en in het laatste domein om meer generieke. Let wel, de drie pijlers gelden onverkort voor het totale IT-veld ongeacht het toepassingsgebied. Daarbij bestaat een natuurlijke spanning tussen de afzonderlijke pijlers. Beveiliging en continuïteit zijn voor de krijgsmacht leidend. De invoering van innovatieve toepassingen zal dus altijd eerst aan deze pijlers worden getoetst.

Voor alle pijlers is het aspect kosten een bepalende randvoorwaarde. Met deze visie is IT niet meer een *cost driver* maar een essentiële *enabler* voor de operatie en de bedrijfsvoering. Dit sluit natuurlijk niet uit dat budgetten gelimiteerd zijn en dat de toepassing van IT altijd moet plaatsvinden binnen de beschikbare financiële ruimte.

Tot slot is voor het vinden en handhaven van de balans tussen de drie pijlers en het aspect kosten een heldere *governance* inclusief *control framework* een voorwaarde. De behoeftesteller (de Commandant der Strijdkrachten in de *demand* rol), het ICT-domein (de *supply* rol) en de CIO moeten samen beschikken over algemeen geaccepteerde meetinstrumenten (waaronder IT-audits), indicatoren, processen en *best practices*. Dit schept de voorwaarden voor besluiten in het IT-domein om daarmee de juiste evenwicht te vinden tussen risico en investeren in controle.

2.3 Randvoorwaarden aan de IT van de toekomst

Voor IT als enabler gelden de volgende randvoorwaarden:

- *Optimaal ondersteunend aan het primair proces.* Een responsieve krijgsmacht zoals omschreven in de nota “In het belang van Nederland” vraagt IT-voorzieningen die gericht zijn op de behoeften vanuit het primaire proces, met de nadruk op inlichtingen en commandovoering. De laatste is essentieel voor de krijgsmacht bij haar werk in binnen- en buitenland, ook als niets anders meer werkt.
- *Internationale militaire samenwerking.* De nota *In het belang van Nederland* berust op het uitgangspunt dat Nederland niet in staat is op eigen kracht zijn veiligheid te verzekeren. Onze veiligheidsbelangen zijn verknoopt met de wereld om ons heen. Om dreigingen en risico’s ook in de toekomst het hoofd te kunnen bieden, is verdieping van militaire samenwerking noodzakelijk, zowel apart met gelijkgezinde landen als in multinationaal verband. Dit stelt ook eisen aan de IT; deze moet de interoperabiliteit naadloos ondersteunen.
- *Ondersteunend voor de samenwerking met partijen buiten Defensie.* De toekomstige bedrijfsvoering kenmerkt zich door samenwerking. Samenwerking is een belangrijk middel om een balans te vinden tussen kosten, toegang tot innovatieve oplossingen en behoud van capaciteiten voor de krijgsmacht. Samenwerking speelt een belangrijke rol in de discussie over het verwerven en vervangen van basis- of nichecapaciteiten. IT moet geschikt zijn om veilig en betrouwbaar gegevens uit te wisselen en procesketens tussen samenwerkende partijen te verbinden.
- *Flexibel, uitbreidbaar en betaalbaar.* De krijgsmacht als geheel moet veelzijdig en betaalbaar zijn. Dat legt aan IT de randvoorwaarden flexibiliteit, uitbreidbaarheid en betaalbaarheid op.
- *Standaardisatie.* Waar mogelijk worden vergelijkbare processen gecombineerd, gestandaardiseerd en ingericht conform *best practices* waarbij IT leidend is. Alleen bij zwaarwegende redenen kan daarvan worden afgeweken.
- *Uniform en geïntegreerd tijdens vredesbedrijfsvoering en operationele inzet*. In de bedrijfsvoering streeft Defensie naar vereenvoudiging en integraliteit. Bedrijfsprocessen vormen geïntegreerde ketens. Processen in de bedrijfsvoering zijn zoveel mogelijk gelijk aan processen tijdens operationele inzet *(train as you fight)*. Dit vereist IT die defensiebreed uniform werkt en voldoende geïntegreerd is om gegevens onder alle gebruiksomstandigheden veilig en betrouwbaar uit te wisselen.
- *Kort-cyclische en kleinschalige ontwikkelingen.* Om de snelle ontwikkelingen van IT ten volle te kunnen benutten, is ook een bijbehorende sturing, planning en projectvoering nodig. Het credo is uitgaan van kort-cyclische ontwikkelingen en het steeds weer bijsturen op basis van actuele ontwikkelingen. De krijgsmacht moet zich ook meer richten op het assembleren van IT-modulen tot een werkend geheel. Deze wijze van ontwikkelen en assembleren vraagt meer flexibiliteit en specifieke kennis. Met deze randvoorwaarde moet ook rekening worden gehouden in de plannings- en begrotingscyclus.
- *De gebruiker staat centraal.* De gebruiker van IT-voorzieningen staat centraal. Hij/zij moet kunnen beschikken over de juiste informatie die nodig is om de opgedragen taken uit te voeren, in de goede vorm en op het gewenste moment. Daarvoor formuleert de behoeftesteller, gehoord de gebruikers, ook een duidelijke opdracht die is toegespitst op de relevante operationele gebruikscondities.
- *Samenwerking in de keten*. De *demand*- (de Commandant der Strijdkrachten) en de *supply*functie (de leverancier van IT-diensten) dienen, gezien deze randvoorwaarden, intensief samen te werken om de IT van de toekomst verder door te ontwikkelen. De CIO reikt de kaders aan waaronder dit moet gebeuren.

3. De pijlers nader uitgewerkt

Samen vormen de pijlers “continuïteit, beveiliging en innovatie” het fundament waarop de IT van de krijgsmacht wordt gebouwd. De volgende paragrafen bevatten een uitwerking van elk van de pijlers.

3.1 Continuïteit

Het huidige en toekomstige optreden van de krijgsmacht vereist dat de essentiële functionaliteit van IT voor de commandovoering over de hele keten van *sensor* naar *effector* kan worden ingezet, ongeacht of dit optreden in een inzetgebied of binnen Nederland plaatsvindt. IT maakt mogelijk dat inlichtingen, sensorwaarnemingen vanuit (on)bemande systemen en waarnemingen door uitgestegen militairen combineerbaar zijn tot geïntegreerde informatie voor *Situational Awareness / Situational Understanding* en een *Common Operational Picture.* De krijgsmacht is hiermee sterk afhankelijk van IT. Daarbij is de krijgsmacht de “zwaardmacht” van de de BV Nederland. Met andere woorden, als niets meer werkt moet onze organisatie haar werk kunnen voortzetten. Dit geldt in binnen- en buitenland. Continue IT-voorzieningen zijn dan ook noodzakelijk om dit te ondersteunen.

Any time, any place, any device: hiermee wordt het vermogen bedoeld om informatie op elke plaats en tijdstip in de door de gebruiker gewenste vorm beschikbaar te hebben (dit kunnen defensiegebruikers zijn of gebruikers van organisaties waarmee wordt samengewerkt). Ook kan een defensiemedewerker de ene dag op een kazerne werken en de andere dag in een missiegebied. De toegang tot de data moet dan ook gegarandeerd zijn. *Devices* bestaan niet alleen los, maar kunnen ook onderdeel zijn van bijvoorbeeld een wapensysteem.

Open bronnen en sensoren zorgen voor een constante toename van data *(big data)*. Deze data moeten worden opgeslagen, geanalyseerd en beschikbaar worden gesteld. De IT moet geschikt zijn om uit alle beschikbare bronnen de data te filteren en om te zetten in relevante informatie, ofwel de gebruiker krijgt alleen datgene aangereikt wat nodig is om zijn/haar taak effectief uit te kunnen voeren. IT moet ook in staat zijn de data zelfstandig en geautomatiseerd te analyseren zodat de gebruiker proactief wordt ondersteund bij de uitdagingen waar hij/zij mee wordt geconfronteerd en die hem/haar ook in staat stelt te anticiperen op ontwikkelingen.

Voor de medewerkers van Defensie is in de toekomstige IT een digitale persoonlijke uitrusting beschikbaar voor effectieve en veilige communicatie, samenwerking en informatieuitwisseling. Tevens worden de gebruikers van IT ondersteund met middelen om teams met elkaar te verbinden, rekening houdend met de behoeften van doelgroepen *(communities of interest)* en genetwerkt samenwerken (GSW). De IT voorziet in tijd-, plaats-, en *device*-onafhankelijk werken en de presentatie van IT *(userinterface)* is afgestemd op de taak en de omstandigheden van de IT-gebruiker of zijn/haar rol in een proces. Daarmee is de kwaliteit in termen van gebruiksgemak en ondersteuning van de dagelijkse werkzaamheden gegarandeerd. Beheeractiviteiten van IT zijn op gebruikersniveau minimaal.

Tegen de achtergrond van een sterk innoverende IT, impliceren deze ontwikkelingen dat de continuïteit van IT gegarandeerd moet zijn en blijven: *IT is als het ware het kloppend hart van de organisatie.*

Gebaseerd op het voorgaande gelden de volgende uitgangspunten voor continuïteit:

- Cruciale IT-infrastructuur wordt op basis van redundantie en replicatie uitgevoerd. Deze moet blijven werken en ingezet kunnen worden tijdens omstandigheden waarin reguliere civiele infrastructuren (voor kortere of langere tijd) niet meer beschikbaar zijn.
- De IT-*governance* evenals de uitvoerings- en regieorganisatie worden versterkt.
- IT ondersteunt alle vormen van operationele inzet en is geschikt voor uitwisseling met vertrouwde partners (*joint*, internationaal, *multi-agency*, industrie en publiek) in steeds wisselende combinaties.
- De IT van Defensie is zo ontworpen dat er geen afhankelijkheid is van een enkele leverancier (geen *vendor lock-in*), tenzij dit niet anders kan (bijvoorbeeld integrale wapensystemen).

- Defensie beschikt zelf altijd over toereikende vitale en strategische[3] IT-kennis, capaciteit en expertise op alle relevante niveaus in de organisatie.
- *Sourcing* is een middel en geen doel op zich. Niet strategische activiteiten kunnen in aanmerking komen voor *outsourcing*, strategische activiteiten kunnen in aanmerking komen voor andere *sourcings*vormen zoals samenwerking.

3.2. Beveiliging en Integriteit

De IT moet gegarandeerd betrouwbaar [4] zijn. Alleen op basis van betrouwbare informatie kan besluitvorming en bevelvoering plaatsvinden. Defensie maakt in haar informatievoorzieningsproces gebruik van alle vormen van gerubriceerde- en privacygevoelige gegevens. Het is daarom essentieel dat de beveiliging van deze (opgeslagen) gegevens op orde is en blijft.

Betrouwbare IT is een basis voor samenwerking met derden. Defensie moet veilig kunnen samenwerken met vele partners onder wisselende omstandigheden en mag het gestelde vertrouwen niet beschadigen door continuïteit- of veiligheidsrisico's. Defensie moet daartoe zorgvuldig omgaan met de informatie die partners met haar delen en tevens aantonen *in control* te zijn.

Defensie maakt keuzes over de betrouwbaarheid en robuustheid van IT op basis van risicomanagement en snel veranderende dreigingsbeelden. De digitale weerbaarheid van Defensie wordt tenminste op peil gehouden conform wettelijke kaders en richtlijnen en eisen van partijen waarmee wordt samengewerkt.

Defensie is zelf eigenaar van – of voert vergaande regie over – cruciale strategische onderdelen van de IT. Calamiteitenplannen en continuïteitsplannen borgen de continuïteit zodat bij ernstige verstoringen de bedrijfsvoering zoveel als mogelijk doorgang kan vinden.

Gebaseerd op het voorgaande gelden de volgende uitgangspunten voor beveiliging en integriteit:
- Defensie heeft de beschikking over voldoende cyber expertise om proactief en reactief te handelen bij digitale dreigingen. Waar nodig kan gebruik worden gemaakt van externe expertise, maar altijd onder eigen regie.
- Defensie ontwikkelt en hanteert een expliciet IT beveiligingsbeleid om een goede balans te vinden tussen samenwerking met de markt, het gebruik van nieuwe innovatieve ontwikkelingen en de noodzakelijke beveiliging van haar kernactiviteiten.
- Infrastructuur die als vitaal is geïdentificeerd is en blijft in eigendom van Defensie.
- Partners waarmee wordt samengewerkt beschikken over de door de Beveiligingsautoriteit (BA) en MIVD vereiste beveiligingsniveaus.
- (Wapensysteemgebonden) IT moet voldoen aan nationale en internationale kwaliteitseisen en standaarden.

3.3. Innovatie

Defensie is een organisatie met een grote behoefte aan *high-tech* innovatieve oplossingen. Op het gebied van IT moet Defensie beheerst mee bewegen met snel veranderende omstandigheden in zowel politiek, militair, maatschappelijk als technologisch opzicht. Innovatie beperkt zich hierbij niet tot het geïsoleerd introduceren van nieuwe technologieën ter ondersteuning van de informatiebehoeften, maar vereist het onlosmakelijk inpassen daarvan in de bedrijfsprocessen, opleiding, training, operationele inzet en de commandovoering. Met IT als onlosmakelijk geïntegreerd onderdeel van de bedrijfsvoering innoveren ze als geheel waarbij ze elkaar naadloos versterken.

[3] De wijze waarop vitaal en strategisch wordt bepaald is onderwerp van de strategie.

[4] Onder betrouwbaarbaar wordt een samenstal van kwaliteitsbegrippen verstaan: integriteit, exclusiviteit en beschikbaarheid conform beveiligingsbeleid, onweerlegbaarheid conform kaders m.b.t. *compliancy* en tijdiheid en juistheid vanuit gebruikersoptiek.

Daarbij zoekt de Defensie altijd naar een balans tussen het toepassen van recente en beproefde technologieën en het zich opstellen als *early adopter*. Innovativiteit wordt daarom altijd in samenhang beschouwd met beveiliging en continuïteit. Voor beproefde technologieën zal Defensie zoveel als mogelijk gebruik maken van *open source* en open standaarden onder het principe van *comply or explain*.

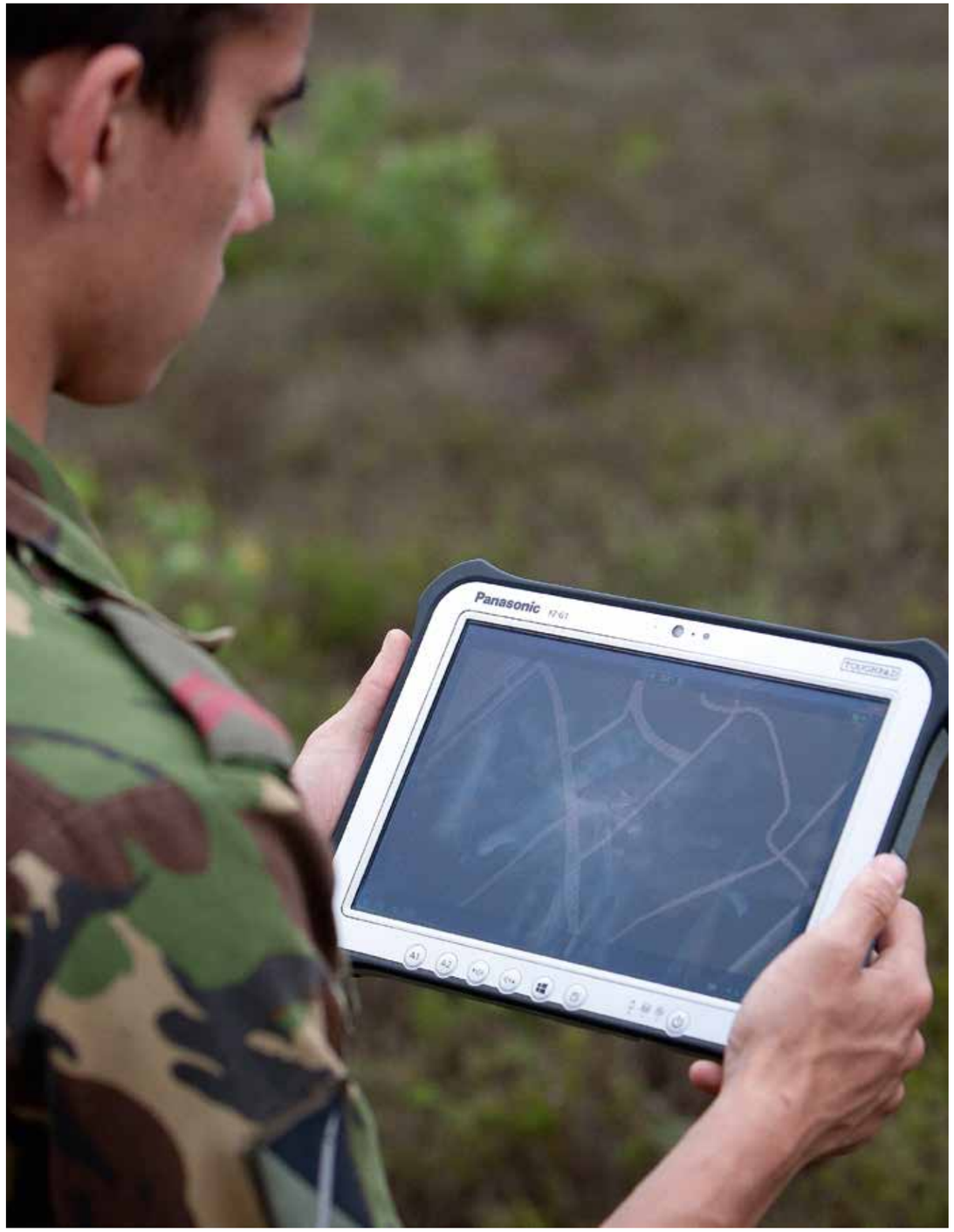
Op deze wijze beschouwt Defensie IT ook als een belangrijk hoofdwapensysteem en daarmee een *enabler* voor innovatie. Kleinschalige beproevingen en *Concept Development and Experimentation* (CD&E) worden ingezet om de toegevoegde waarde van nieuwe mogelijkheden van IT aan te tonen.

Kennis, kunde en ervaring zijn naast de al genoemde punten het fundament van elke succesvolle innovatie. Defensie zal haar rol van "alle kennis en kunde in huis" moeten transformeren naar "alle kennis en kunde van ketenpartners en marktpartijen kunnen mobiliseren, integreren met de noodzakelijke eigen kennis en kunde, en regisseren" om alle veranderingen te kunnen volgen. Intensieve samenwerkingsverbanden met kenniscentra en de industrie zijn hiervoor noodzakelijk. De onderdelen van de verschillende partijen waarmee wordt samengewerkt moeten één werkend geheel opleveren. Defensie is hiervoor eindverantwoordelijk en borgt de integratie. De IT van de toekomst moet ook voldoende flexibel zijn om nieuwe technologie in te passen en te beproeven en vervolgens breder beschikbaar te stellen.

Er is niet één allesomvattend informatiesysteem dat alle informatiebehoeften van Defensie invult. De IT zal op het niveau van de informatiesystemen een hybride stelsel van verschillende oplossingen zijn (zoals oplossingen van marktpartijen, Rijk of NATO). Het technische fundament is echter grotendeels gestandaardiseerd voor de diensten die Defensie levert. Als aanvulling op grote proces ondersteunende systemen zoals ERP worden op elkaar afgestemde standaardpakketten en services gebruikt. Kortom, de geïntegreerde bedrijfsvoering wordt ondersteund door een stelsel van goed samenwerkende IT-modulen. Deze modulen kunnen los ont-wikkeld worden, maar moeten altijd passen binnen de Defensie IT-architectuur.

Voor het optimaal samenwerken van de verschillende delen van de IV wordt een overkoepelende service gerichte architectuur (SGA) ontwikkeld en ingezet. Ten slotte wordt het concept van de basisregistraties verder ontwikkeld en wordt het gegevensbeheer verder verbeterd waardoor de kwaliteit van de informatie toeneemt.

Gebaseerd op het voorgaande gelden de volgende uitgangspunten voor innovatie:
- Defensie werkt zoveel als mogelijk met open *source* en open standaarden. Hier geldt het *comply or explain* principe.
- Defensie beschikt (eventueel samen met partners) over IT innovatiecentra voor de ontwikkeling van strategische IT.
- De IT van de toekomst is geschikt voor samenwerking met beveiligde koppelingen.
- Management en medewerkers worden actief getraind in het effectief gebruiken van steeds nieuwe toepassingen van IT.



4. Tot slot

Om optimaal te kunnen inspelen op de steeds sneller veranderende wereld, maakt IT het verschil. Dat is de kernboodschap van deze visie. Defensie streeft daarom naar een flexibele bedrijfsvoering ondersteund door een innovatieve IT waar continuïteit, beveiliging en integriteit vanzelfsprekend zijn. Defensie zoekt daarbij naar een balans tussen het toepassen van de meest recente en beproefde technologieën en het zich opstellen als *early adopter*. Daarmee wordt innovatie altijd in samenhang met beveiliging en continuïteit beschouwd.

Het huisvesten van onze IT op de drie pijlers vraagt ook wat van onze (toekomstige) partners. Daar waar grote marktpartijen gericht zijn op met name continuïteit en grootschalige beheersmatige ondersteuning, zijn in de regel kleinere marktpartijen doorgaans meer gericht op innovatie. Defensie zoekt de samenwerking dan ook in een combinatie van beide.

Op termijn zal de IT van Defensie zich transformeren van een samenstel van infrastructuur en applicaties naar een virtueel stelsel dat als service de operaties en de bedrijfsvoering naadloos en actief ondersteunt. De gebruiker zoekt in deze omgeving niet meer zelf naar de applicatie die gaat helpen bij de uitvoering van de opdracht, maar krijgt de benodigde informatie als het ware vanzelf aangereikt. Dat is het wenkende perspectief van onze IT!


L801