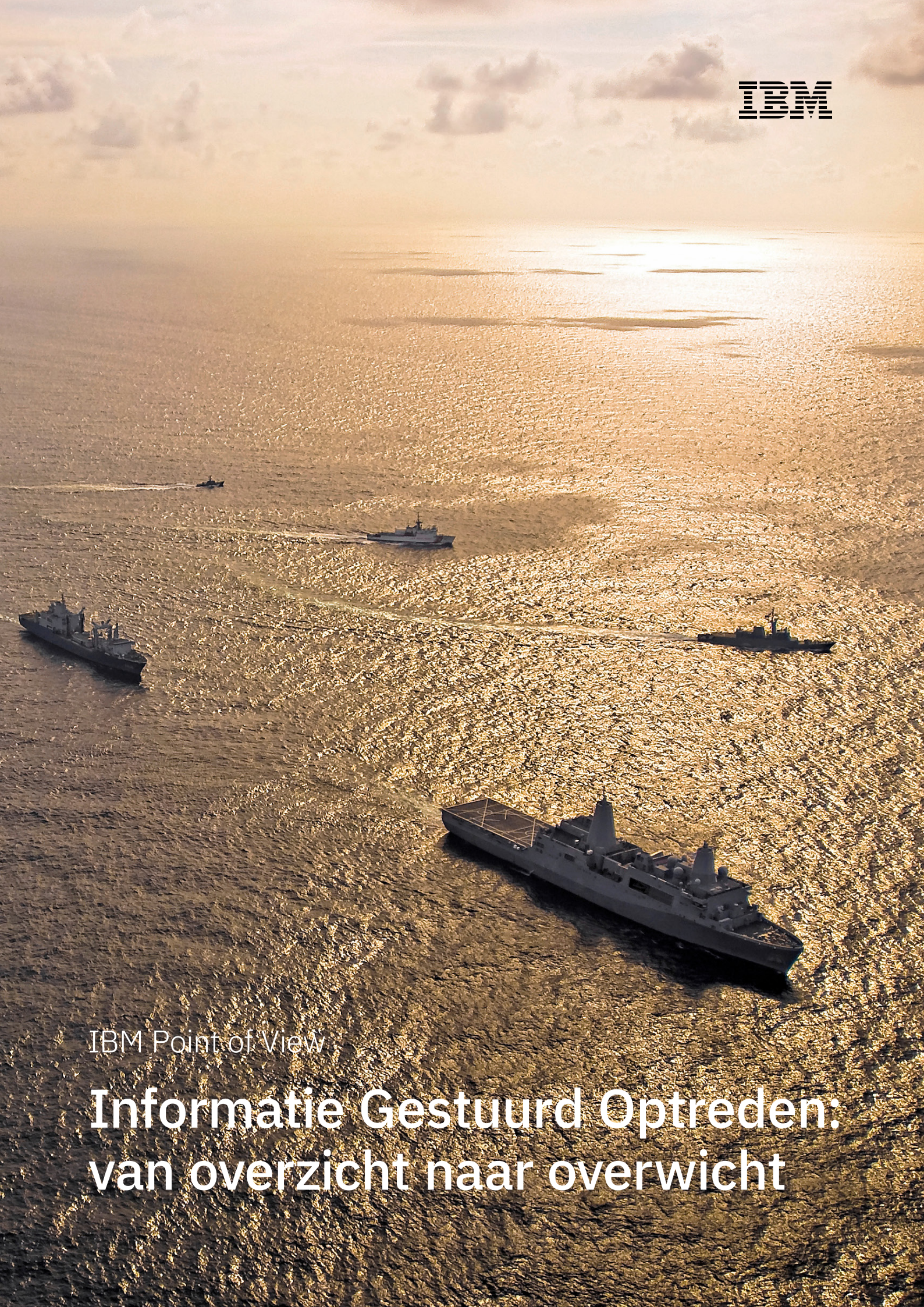


IBM Point of View

Informatie Gestuurd Optreden: van overzicht naar overwicht



Inhoud

Veranderingen voor de militair zijn steeds ingrijpender 5

Informatie maakt het verschil 5

Traditionele aanpak leidt niet tot succes 6

Toewerken naar informatiedominantie 7

De drie uitdagingen bij de transitie naar informatiedominantie en IGO 10

Uitdaging 1: 12
kwetsbare verouderde IT-backbone

Uitdaging 2: 14
verhogen van de informatiegereedheid

Uitdaging 3: 16
een organisatie die ingericht is op adoptie van innovatie

Bijlage 18



Veranderingen voor de militair zijn steeds ingrijpender

Voor Defensie is de wereld een steeds veranderlijker plek; bedreigingen voor vrede en veiligheid zijn minder traditioneel, onvoorspelbaarder en manifesteren zich op meer domeinen zoals cyber en het grensvlak van civiel en militair.

De druk op Defensie om adequaat te kunnen antwoorden op deze veranderingen wordt groter; in de Defensienota is te lezen dat het ministerie inzet op het gebruik van 'Informatie Gestuurd Optreden' (IGO). Dat komt tot uiting in investeringen in de integratie van informatiebronnen, het onderling veiliger en sneller delen van informatie en de verdergaande samenwerking met civiele en internationale partners. Hoe kan Defensie het maximale uit deze investeringen halen: welke middelen om informatie te delen hebben prioriteit, welke technologie is daar geschikt voor en welk stappenplan leidt naar een perfect functionerend wapensysteem op basis van IGO? In dit document gaan we daar nader op in. Om uiteindelijk antwoord te geven op de vraag: hoe kan Defensie 'informatie' als wapensysteem op basis van IGO vormgeven en inzetten?

Informatie maakt het verschil

Militairen op een missie verwachten niet anders dan dat de relevante informatie tijdig, veilig en compleet op het best geschikte medium (smartphone, laptop, C2-displays) beschikbaar komt. Afhankelijk van domein en onderdeel zal de informatiebehoefte en presentatie verschillen; ook hier spelen tijdigheid, volledigheid en flexibiliteit een belangrijke rol.

Enkele voorbeelden van specifieke informatiebehoeften:

- De F35-vlieger die verkenningen uitvoert voor een internationale vredesmissie in het Midden-Oosten moet informatie tegelijkertijd kunnen delen met diverse partijen. Bijvoorbeeld met het marinefregat in de Perzische Golf en de civiele havenautoriteiten bij het signaleren van verdachte scheepsbewegingen. Op hetzelfde moment moet deze vlieger op de hoogte worden gesteld bij een verhoogde cyberdreiging die wellicht de beveiligde communicatie met de basis kan verstoren.
- Een militaire inlichtingenanalist wil snel diverse gegevensbronnen en analyses kunnen koppelen en relateren aan elkaar om een verdacht persoon te traceren.
- De pelotonscommandant van de infanterie bij vredesoperaties in Irak wil goed inzicht hebben de tactische situatie: hoe ziet het terrein eruit, waar kan drukte verwacht worden en waar is er verhoogd risico op IED's? Waar bevinden zich mogelijk terroristische cellen en hoe is het sentiment onder de bevolking?

Bij het laatste voorbeeld is er zelfs een verband tussen de informatiebehoefte van de inlichtingenanalist en de militairen op missie. Kortom, Defensie moet de militair en de missie centraal stellen in het verzorgen van een snelle en adequate informatievoorziening. Daarbij moet het

betrokken militair personeel alle informatie van de verschillende eenheden – op land, in de lucht of op zee – beveiligd kunnen combineren en delen met elkaar en met derden.
Hoe adopteren we doctrines waarin informatie belangrijker wordt dan elk ander traditioneel, beschikbaar militair middel? Dat is de uitdaging waar Defensie voor staat. De informatiepositie bepaalt welke course of action gekozen wordt. Daarnaast bepaalt de mate waarin Defensie die informatiepositie kan actualiseren en verbeteren of van deze course of action moet worden afgeweken en welke alternatieven moeten worden overwogen.
De informatiepositie bepaalde altijd al in hoge mate de uitkomst van een militair conflict; niet of er meer of betere militaire macht wordt ingezet. Maar deze informatiepositie is tegenwoordig meer dan ooit vluchtig, divers en afhankelijk van technologie. Daarbij is de huidige informatiepositie voornamelijk afhankelijk van de toegang tot de juiste technologie, de achterliggende gegevens en de integrale benadering om alle benodigde data te verkrijgen.

Traditionele aanpak leidt niet tot succes

Bij traditionele technologische doorbraken is de maatschappij, en dus ook Defensie, gewend om de middelen centraal te stellen. Denk aan een nieuw jachtvliegtuig, een nieuw communicatiemiddel en nauwkeurigere sensoren. Dat zijn bekende voorbeelden waarmee in het recente verleden Defensie de volgende generatie militaire conflicten het hoofd bood.

Het nadeel van het centraal stellen van middelen is dat deze werkwijze vaak slechts een deelprobleem oplost en tegelijkertijd de complexiteit van de militaire werkomgeving vergroot. Een aanpak die gericht is op het beter laten samenwerken van die middelen en op het integreren van bestaande informatiebronnen leidt tot een effectievere inzet en hogere kans op succes.

De uitdaging ligt voornamelijk op het gebied van (strategische) flexibiliteit: hoe kunnen we informatie en middelen slim integreren en combineren? En hoe snel kunnen we daarin variëren als de situatie daarom vraagt? Kan een eenheid mariniers die op het punt staat een amfibische landing uit te voeren op een onbekende kust het aanvalsplan aanpassen op basis van satellietbeelden, gecombineerd met inlichtingen van de MIVD? Zodat ze bijvoorbeeld later of eerder tot actie overgaan of een andere uitrusting meenemen?

Met andere woorden: IGO is gebaseerd op het maximaal benutten van het informatiepotentieel. Dit noemen we in het vervolg van dit document informatievoordeel of informatiedominantie. Dit is cruciaal voor succes op tactisch, operationeel en strategisch niveau. Dat geldt zowel voor de eenheden die de missie uitvoeren als voor het ‘bedrijf defensie’ daarachter. De achterliggend organisatie dient immers de gereedstelling en bedrijfsvoering informatiegestuurd in te richten zodat Defensie de informatiedominantie op langere termijn kan voortzetten.

Toewerken naar informatiedominantie

Informatiedominantie is dus essentieel bij IGO: eenheden moeten de opponent een stap voor kunnen zijn, op basis van de betere informatiepositie. Daardoor kan de eenheid beter en sneller het besluit nemen tot actie. Informatiedominantie betekent dat de eigen eenheid zowel meer als betere informatie tot zijn beschikking heeft dan de opponent. Ten tweede moet deze informatie tijdig en actueel zijn. Ten derde dient deze informatie relevant te zijn in de context van die eenheid.

De impact van IGO op gereedstelling en voortzettingsvermogen is eveneens groot. Denk aan verbeterde materiele gereedheid door middel van predictive maintenance. Of aan het beschikbaar hebben van informatie over personeel, logistiek en trainingen voor eenheden die op het punt staan naar operatiegebieden te vertrekken. In dat geval kan Defensie alle mogelijke beschikbare data gebruiken bij missieplanning en -voorbereiding.

Wij onderscheiden vier pijlers van informatiedominantie:



- **Volledigheid. Ofwel:** een zo compleet mogelijk beeld van de situatie. Dit is afhankelijk van de fase van de missie, de omvang en complexiteit van het domein en allerlei externe factoren. De beperkende factor is de toegang tot informatie: kunnen alle gegevensbronnen die dit complete beeld vormen, benaderd worden? Bij een tactische situatie speelt bijvoorbeeld de beschikbare bandbreedte een rol. Dan moet er gekozen worden welke gegevens uitgewisseld worden. Wilt u bijvoorbeeld wel de locatie van vijandige troepen tonen maar niet de videofeed van de satelliet of drone die deze troepen monitort? Daarnaast is volledigheid afhankelijk van regelgeving en procedures, bijvoorbeeld als gevolg van rubricering; een operator kan op basis van zijn of haar security clearance niet alle beschikbare informatie benaderen.

- **Tijdigheid.** Hierbij draait het om het op tijd verkrijgen van actuele informatie. Ook de tijdigheid van informatie is afhankelijk van de fase van een missie; moet de informatie een eenheid binnen weken, dagen, uren, minuten of zelfs seconden bereiken? En is de informatie nog waardevol na een uur, dag of week? Op strategisch niveau spelen hier heel andere ordegrootten dan in de tactische situatie. De beperkende factor is snelheid;

hoe snel kan je veranderde gegevens distribueren aan de ontvangers? Defensie moet bijvoorbeeld de locatie van een vliegende vijandelijke helikopter real-time kunnen doorgeven aan grondgebonden luchtafweer. Tegelijkertijd moet de gereedheidsinformatie van eenheden snel beschikbaar zijn, ook op stafniveau om de inzet te kunnen plannen of aan te passen.

- **Relevantie.** Hoe zorgt u dat u alleen die informatie verzamelt en presenteert die relevant is voor de situatie op dat moment? Dit is een delicate balans. Aan de ene kant kan een missend detail doorslaggevend zijn. Aan de andere kant moet u waken voor een informatieoverload. Een eenheid wil bijvoorbeeld niet alle vliegende objecten in een straal van 10 km zien, maar alleen de vijandelijke of ongewenste objecten. De beperkende factor is het filteren. Ofwel, hoe goed kan de gebruiker selecteren welke informatie aan hem of haar wordt gepresenteerd?

- **Vertrouwen.** Wat is de mate van betrouwbaarheid van de informatie? Hoe kan een operator op een marinefregat zeker zijn dat de zojuist ontvangen doelinformatie daadwerkelijk door die bevriende eenheid is verstuurd? Hoe goed zijn maatregelen ten aanzien van spoofing en andere vormen van hacking? Validatie is hierbij de beperkende factor; hoe goed en hoe snel kan de operator de betrouwbaarheid van informatie valideren?

Met de huidige technologie kan de militair steeds beter geïnformeerd worden: hij of zij krijgt snel genoeg, voldoende informatie. Door gebruik te maken van geavanceerde analysemethoden krijgt de militair alle relevante informatie te zien. Voortaan kan de militair filteren en zo een informatieoverload voorkomen. Dus het informatieverwerkende vermogen van de mens is niet langer de beperkende factor.

Voorbeeld: 5th Generation Airforce

Bij de IGO-introductie kijkt de luchtmacht vooral naar verbeteringen in het luchtoptreden, o.a. door de inzet van nieuwe concepten in Command & Control. Daarbij moet de focus liggen op het verbeteren van de Situational Understandig en Awareness tijdens de strategische en operationele missiefase. Dat resulteert in meer flexibiliteit en slagkracht in het tactische domein. Het uitgangspunt is om een centraal aangestuurd luchtoptreden meer en meer los te laten en op drie terreinen te decentraliseren:

- Collaboratie: het aangaan van ad-hoc samenwerkingsverbanden op het moment dat dit relevant is; met andere vliegtuigen maar ook met grond- en zee-eenheden.
- Communicatie: het joinen van tactical data- en voice-networks als daar behoefte aan is, zonder omslachtige procedures voor het overgaan van en naar die netwerken.
- Aansturing (Control): sensoren en actoren in een tactisch netwerk kunnen onafhankelijk van elkaar opereren, in een demand-supply model zonder een centrale aansturing.

Gegevensbronnen die de luchtmacht hiervoor kan raadplegen zijn combinaties van satelliet- en andere geogegevens van de omgeving, informatie uit het intelligence-domein en gegevens van andere vliegtuigen/UAV's die de laatste updates hebben over die regio. De gegevensbronnen zijn legio. Dat vereist bepaalde filtercapaciteit van de vlieger. Helaas is de vlieger vaak zelf niet in staat om deze data te interpreteren en in het geheel te plaatsen.

In dat geval kunnen zelflerende systemen die deze filtercapaciteit bezitten helpen. Deze voorzien de vlieger van relevante inzichten. Op basis daarvan kan hij of zij gefundeerde besluiten nemen om tot de juiste actie over te gaan. Bovendien vergroot een dergelijk systeem de autonomie van een vlieger ten opzichte van het huidige gecentraliseerde Command & Control-principe. Met als resultaat meer slagvaardigheid van het luchtoptreden.

De drie uitdagingen bij de transitie naar informatiedominantie en IGO

Wij zien op dit moment drie uitdagingen bij het toewerken naar informatiedominantie en de daaruit voortvloeiende IGO- werkwijze.

1. IT is robuust en digitaal weerbaar

IGO vereist een sterke, veilige en moderne 'IT-backbone' als fundament. Waarom? Een verouderde infrastructuur, zowel statisch als ontplooid en in het mobiel tactische domein, is kwetsbaar. Deze kan niet de benodigde volledigheid en snelheid bieden. Op dit moment is de infrastructuur bij Defensie geadresseerd als verbeterpunt via programma's zoals GrIT, Foxtrot, VoSS en andere programma's.

2. IT is interoperable en datagedreven

Op dit moment is het lastig om de juiste gegevens te verkrijgen op het moment dat die nodig zijn; veel data zijn gedistribueerd toegankelijk voor militairen als kopieën van de originele set. Bovendien worden deze gegevens meestal niet regelmatig bijgewerkt. Voorbeeld hiervan is de geo-informatie. Deze is vaak weken of maanden oud, terwijl er behoefte is aan real-time informatie over een bepaald gebied, bijvoorbeeld na het overtrekken van een orkaan. Gedateerde informatie vergroot de kans op foutieve beslissingen over de inzet van militaire eenheden. Daarnaast is het met een verouderde infrastructuur vaak moeilijk om goed gegevens te delen met eenheden buiten de traditionele partners. Land-, lucht- en zee-eenheden kunnen hun gegevensset slechts deels onderling delen. Dit probleem wordt nog duidelijker bij het delen van informatie met buitenlandse eenheden of civiele partners. Dat is niet alleen een technische uitdaging, maar ook op het vlak van processen en cultuur.

3. IT is wendbaar

Een moderne defensieorganisatie moet zich nieuwe technologieën en IT-innovaties, zoals voor gegevensanalyse, snel eigen kunnen maken. De ontwikkelingen op dat gebied gaan zo snel dat het essentieel is om de eigen organisatie te hervormen –en wel zodanig dat het adopteren van nieuwe technologieën een 'tweede natuur' wordt. Alleen dan kan Defensie het mogelijke voordeel dat tegenstanders ontwikkelen met behulp van nieuwe technologie snel elimineren. Sterker, de defensieorganisatie kan een asymmetrisch en strategisch voordeel behalen door deze technologieën reeds te hebben ontwikkeld voordat mogelijke tegenstanders dat hebben kunnen doen. Denk hierbij aan het inzetten van autonome voertuigen en drones, geavanceerde AI-middelen om dreigingen in kaart te brengen of aan moderne cyberdefensietechnologieën.

Wat is het antwoord op elk van de drie uitdagingen op weg naar informatiedominantie en de daaruit voortvloeiende IGO-werkwijze? In de volgende paragrafen gaan we daar per uitdaging dieper op in.

Voorbeeld: IGO bij de Koninklijke Marine

In 2020:
De regering besluit om een fregat naar de Straat van Hormuz te sturen. In allerijl wordt het schip gereedgemaakt voor deze taak. Het leveren van bemanning, onderdelen, munitie, brandstof en andere voorraden krijgt per direct de hoogste prioriteit binnen de betrokken marineorganisaties. Wat betekent dat voor de andere eenheden en taken van de marine? Dat is nog niet duidelijk. Dit maakt het onmogelijk om alternatieven te overwegen. Zodra het schip is vertrokken richting de Straat van Hormuz, wordt onderweg nog hard geoefend om de operationele gereedheid van het fregat te vergroten. Daarnaast wordt in kaart gebracht welk effect deze ad-hoc inzet heeft op de gereedheid van de andere marine-eenheden. Vervolgens wordt dit gerapporteerd aan de marineleiding.

In 2030:
Door de integrale informatiepositie van de marineleiding (OPS) in de gereedheid en inzetbaarheid van marine-eenheden, is het mogelijk om ad-hoc inzetverzoeken te analyseren en alternatieven te overwegen. Ook is het direct helder welke impact het verschuiven en prioriteren van de inzet heeft op andere eenheden. Dit geldt zowel voor de impact op de personeelsgereedheid en geoefendheid als voor de materiele gereedheid en de voorraadposities. Bij langere inzet of het ‘rouleren’ van eenheden is die planning beter te maken. Bij het plannen tijdens de operatie maakt een marine-eenheid gebruik van diverse bronnen binnen en buiten de marine of Defensie, zoals bijvoorbeeld de NAVO of EU.

Uitdaging 1: kwetsbare verouderde IT-backbone

IT is robuust en digitaal weerbaar

De militair moet gegevens die cruciaal zijn voor zijn of haar missie kunnen inzien. Dit vereist een IT-infrastructuur die aan de ene kant robuust en veilig is. Aan de andere kant moet de infrastructuur goed toegankelijk zijn voor gebruikers, ongeacht hun device en verbindingsmogelijkheden. Hoe bouw je een infrastructuur die aan beide eisen voldoet? Definieer deze aan de hand van de volgende ontwerpprincipes:

1. **Always-on** – Defensie is een 24-uurs bedrijf dat wereldwijd opereert. Daarom moet de IT-backbone altijd beschikbaar zijn. Dat vraagt om een always-on infrastructuur, die voldoende redundant is om storingen en (on)gepland onderhoud op te vangen, zonder dat de continuïteit in gevaar komt.

2. **Any device** – gebruikers moeten met elke device toegang tot de IT-backbone hebben, ongeacht de leverancier en het besturingssysteem. Vanuit security-oogpunt zijn er uiteraard wel beperkingen met betrekking tot de gegevens en applicaties. Daarnaast kan de toegang beperkt zijn in gebieden of situaties met weinig bandbreedte voor gegevenstransmissies. Deze situaties zijn er altijd. Maar deze beperkingen mogen nooit leiden tot een volledig onbereikbare, missie-relevante gegevensset.

3. **Flexibel en schaalbaar** – steeds meer missies en oefeningen van Defensie vinden plaats met ad-hoc coalities van militaire en civiele partijen. Daarom is het essentieel dat de IT-backbone ingericht is op het aangaan van dergelijke coalities. Dit betekent dat er eenvoudig toegang moet kunnen worden verleend. Daarnaast moet Defensie de capaciteit van de infrastructuur eenvoudig kunnen opschalen om deze coalities te faciliteren.

4. **Veilig en federatief samenwerken** –beveiliging van de IT-backbone is essentieel voor militaire operaties en bedrijfsvoering. Deze kan met moderne authenticatie- en autorisatiemechanismen, zoals federatie van netwerken, sterk worden geautomatiseerd zonder concessies aan de veiligheid. Dergelijke automatisering van toegang en beveiliging versnelt ook het besluitvormingsproces en de uitvoering van een missie. Daarnaast moet de IT-backbone ingericht zijn op het detecteren en pareren van moderne cyberaanvallen. Dit is mogelijk door een goede netwerkinrichting inclusief HGI/LGI-koppeling. Denk hierbij ook aan Federated Mission Network (FMN) en Protected Core Network (PCN). In bijlage 1 vindt u meer over de architectuur van deze IT-backbone.

Voorbeeld: IGO bij de Koninklijke Landmacht

In 2020:
Een infanterie-eenheid heeft de opdracht om een middelgrote stad veilig te stellen in voornamelijk onbekend gebied. De uitdaging? Bezet de knooppunten die cruciaal zijn om de verkeers- en informatiestromen te monitoren en te bewaken. Zodat de eenheid met minimale middelen, een maximale controle over de stad krijgt.

Welke posities moeten worden ingenomen? Om dat te bepalen, kijken de commandant en de staf niet alleen naar objectieve en feitelijke informatie, zoals de geografische situatie, maar ook naar de subjectieve informatie. Denk hierbij aan sentimenten bij de bevolking, events die plaatsvinden op social media, verkeersstromen en trends daarin, het risico op gerichte aanvallen van tegenstanders, enzovoorts. En hoe stellen we vast welke middelen de eenheid nodig heeft, zoals wapens, en beschermings- en logistieke middelen? Ook dit wordt grotendeels gebaseerd op subjectieve informatie. Om over zo gedetailleerd en compleet mogelijke subjectieve informatie te beschikken, analyseert de eenheid diverse openbare bronnen, zowel op papier als online. Dit proces is echter traag en onvolledig. Daardoor komt de informatie geregeld versnipperd, onvolledig en te laat binnen bij de commandant van de eenheid.

2025:
De opdracht is hetzelfde, maar de informatievoorziening is veranderd. De eenheid beschikt nu over een integraal totaalbeeld. Compleet en gedetailleerd, gebaseerd op zowel objectieve als subjectieve informatie. Dit beeld wordt dynamisch opgebouwd door geautomatiseerd digitale bronnen te raadplegen, gegevens te verzamelen en combineren. Vervolgens tonen intelligente algoritmes de meest relevante gegevens. De eenheid kan deze integrale dataset benaderen vanaf alle verschillende locaties. Dat betekent dat de staf, eenheden in het veld, militaire en civiele partners deze informatie direct kunnen raadplegen indien nodig. Het voornaamste strategische voordeel? Doordat de commandant over dit soort geïntegreerde informatie beschikt, kan de eenheid de mensen en middelen veel effectiever inzetten en het risico op verliezen minimaliseren.

Uitdaging 2: verhogen van de informatiegereedheid

IT is interoperable en datagedreven

Hoe krijgen we de juiste gegevens op tijd bij de militaire gebruiker? Een traditionele manier is om deze fysiek 'mee te nemen' op missie, bijvoorbeeld in het geheugen van pc's of lokale netwerken – al dan niet ad-hoc missienetwerken in operatiegebieden. In dat geval werden updates hiervan 'batch'-gedreven uitgevoerd: elke dag of week kon een nieuwe update van informatie via diverse kanalen worden uitgevoerd (handmatig, via gegevenslinks, satcom uplinks of andere tijdrovende manieren). Dit helpt de militair niet om de OODA loop te versnellen ten opzichte van de tegenstanders. De militair is immers veel tijd kwijt met het verkrijgen van voldoende kwalitatief hoogwaardige informatie voordat hij of zij tot besluitvorming en actie kan overgaan. Dat vergroot op zijn beurt weer het risico dat acties worden uitgevoerd op basis van te weinig of foutieve gegevens.

Hoe versnel je de informatie-uitwisseling in het veld? Dat vereist optimalisatie van toegang tot de gegevensbron in plaats van het kopiëren en 'meenemen' van de gegevens. Daarnaast moeten gebruikers de gegevens snel en goed kunnen integreren. Ten slotte is het belangrijk deze integratie continu te doorlopen, in een soort oneindige cyclus. Dit verbetert de kwaliteit en de actualiteit van de gegevens – in feite praten we hier over een 'mission datahub'.

Het is dus vooral belangrijk om blokkades tot informatie weg te nemen. Dat kan relatief eenvoudig, omdat blokkades vaak meer procedureel dan technisch van aard zijn. Bij de voorbereiding van een missie kan Defensie hier alvast aandacht aan besteden: welke gegevenssets zijn nodig in het operatiegebied, en voor welke type operatie? Wie is verantwoordelijk voor die gegevens? Hebben wij toegang tot die gegevens en zo nee, verkrijgen we die op tijd en met mandaat? Welke andere (civiele) partners zijn aanwezig in het operatiegebied waarmee we kunnen samenwerken en gegevens kunnen delen? In bijlage 3 leest u meer over een dergelijke missie-datahub.

Het is belangrijk te beseffen dat de ultieme real-time toegang tot de datahub niet altijd mogelijk is vanwege militair-tactische omstandigheden. Denk hierbij aan de missie van onderzeeboten in vijandelijke wateren of special forces eenheden.

De bovenstaande wijze van gegevensdeling en -gebruik leidt tot een hoge informatiegereedheid; een essentieel element in de totale gereedheid van een eenheid. Dit is naast materiële, personele en oefengereedheid van een eenheid, uit te drukken in de mate waarin de eenheid de OODA loop kan versnellen door informatie te delen en te gebruiken.

Voorbeeld IGO Koninklijke Luchtmacht

In 2016:
De F16-vlieger staat klaar voor take-off. Hij of zij heeft alle informatie over de verkenningsmissie boven een aangewezen operatiegebied bij zich in de cockpit. De missie-briefing is hardcopy aan de vlieger overhandigd. Tien minuten na take-off wordt de vlieger door de gevechtsleider geïnformeerd dat zijn of haar assistentie nodig is voor luchtsteun aan grondeenheden omdat deze onder vuur liggen. De locatie is veranderd en de nieuwe aanvliegroute gaat door vijandelijk gebied. Via de radio wordt de vlieger op de hoogte gesteld van het nieuwe doel en de mogelijke vijandelijke gebieden. De vlieger schrijft alles op en bepaalt in de cockpit de nieuwe route, aanvalsplannen en alternatieven op basis van wat hij of zij zojuist heeft gehoord.

In 2025:
De F35-vlieger beschikt voor take-off over alle informatie van de missie in een on-board systeem, inclusief locatie van andere eenheden, verbindingsopties en de waypoints naar het operatiegebied. Bij het veranderen van de missie wordt het systeem ge-update met de nieuwe locatie, route, markering van (mogelijke vijandelijke) gebieden en andere eenheden. Ook versturen de grondeenheden digitaal informatie die aangeeft vanwaar ze onder vuur liggen. Met deze informatie kan de vlieger het tactische plan beter in kaart brengen en uitvoeren, eventueel geadviseerd door een besluitvormings-ondersteunend systeem aan boord.

Uitdaging 3: een organisatie die ingericht is op adoptie van innovatie

IT is wendbaar

Innovatie in het werkveld van Defensie is vaak nog ingericht per krijgsmachtdeel, in een specifiek domein (lucht, land, zee, cyber) en niet altijd integraal. Om zinvol te innoveren is het belangrijk om de hele organisatie zodanig in te richten dat die blokkades worden weggenomen. Daarnaast moet er een cultuur van innovatie ontstaan, waarbij kleine ideeën die goed uitpakken snel kunnen worden opgepakt door de hele organisatie. Het militaire verleden kent een groot aantal voorbeelden van een dergelijke innovatiekracht; helaas wel vaak alleen onder de druk van een gewapend conflict. Het blijkt lastig om in een relatieve vredessituatie een dergelijke 'pressure cooker' te organiseren. Voor de Nederlandse krijgsmacht is het inzetten van innovatie dé manier om met relatief beperkte middelen een strategisch, operationeel of tactisch voordeel te behalen ten opzichte van tegenstanders.

Hoe behaal je voordeel uit innovatie? Laten we een blik werpen op organisaties die wel in staat zijn om een innovatiedrive van binnenuit te vertalen naar tastbare resultaten.

Een belangrijk element bij het benutten van innovatie, is het doorbreken van bestaande organisatiegrenzen. Houd bijvoorbeeld zo veel mogelijk joint- en combined oefeningen en stel de informatiegereedheid (zie voorgaande paragraaf) centraal. Kijk waar er hiaten zijn, hoe die worden opgepakt en hoe de best practices kunnen worden gedeeld met anderen, ook in NAVO- en EU-verband.

Om wendbaar te worden, moet de organisatie wennen aan een constante verandering. Deze continue verbetering van bedrijfsprocessen wordt gedreven door multidisciplinaire, vaak zelfsturende, teams. Zij leveren regelmatig concrete verbeteringen op en integreren deze in de bestaande werkwijze. Zo is direct duidelijk wat de praktijkvoordelen zijn. Bij deze aanpak staan de wensen en behoeften van de individuele militaire gebruiker centraal.

Een andere randvoorwaarde voor een succesvolle realisatie van IGO, is het inrichten van een innovatie-centrische organisatie. De besturing daarvan (zowel Command & Control als bedrijfsvoering) heeft als doel de transformatie van de huidige defensieorganisatie te begeleiden. Dat vereist een andere aanpak dan de traditionele werkwijze.

Een IGO-stuurorgaan is belangrijk om IGO succesvol te implementeren. Door deze in te richten, kan Defensie IGO-initiatieven bij de diverse krijgsmachtonderdelen faciliteren, bijsturen of combineren. Hierdoor kunnen de juiste activiteiten, op het juiste moment en in de optimale volgorde worden uitgevoerd. Bovendien kunnen de verschillende krijgsmachtonderdelen ook gebruik maken van elkaars ideeën, processen en assets.

De inrichtingsprincipes van dit stuurorgaan in hoofdlijnen:

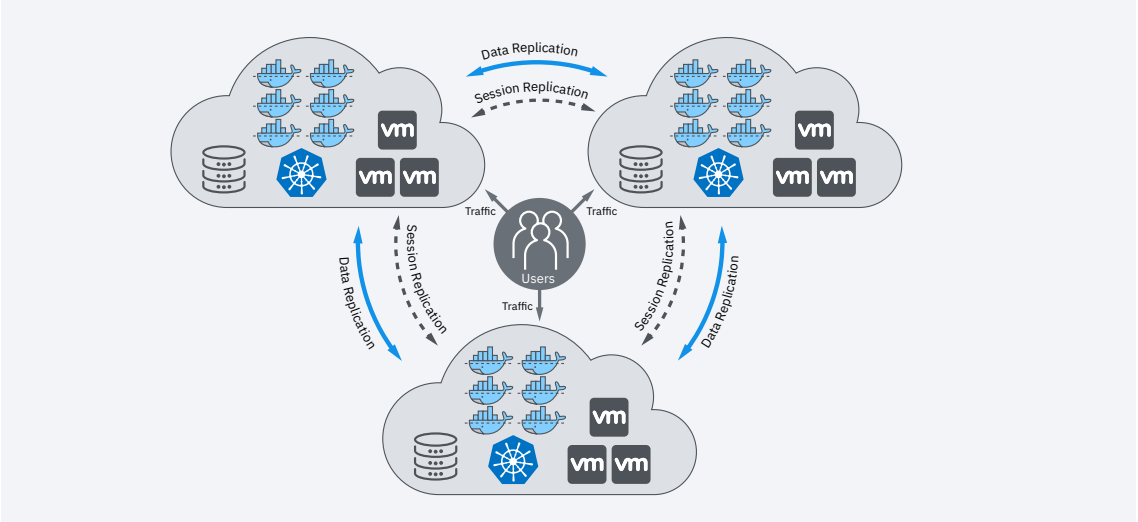
- Vorm volgt functie: organisaties zijn klein, tijdelijk en aanpasbaar. Rollen zijn belangrijker dan functie of rang.
- Verandering is verankerd in directie: er is sprake van een ‘veranderdirecteur’.
- Risicomanagement i.p.v. risicomijding: het is essentieel om risico’s te onderkennen en managen.
- Betrek iedereen bij verandertrajecten: meedenken is niet alleen weggelegd voor ‘veranderkundigen’
- Decentralisatie: spreid de bevoegdheden op het vlak van materieel, logistiek en financiën.

IBM heeft uitgebreide ervaring met het invoeren van innovatieprocessen. Daarbij hanteren we een wereldwijd succesvolle methode. Meer over deze methode vindt u in **bijlage 2**.

Bijlage 1

Always-on, veilige en schaalbare architectuur voor elk device

Een IT-backbone voor zowel statische als ontplooide omgevingen



Het creëren van een robuuste, digitaal weerbare IT-infrastructuur is de eerste stap op weg naar IGO. Hiermee kan Defensie informatie multidisciplinair inwinnen, verwerken en verspreiden. Een van de core principles van het ontwerp is de ‘always-on architectuur’. Dit concept vereist drie IT-omgevingen (gegevenscenters of hardware clusters) waarvan er altijd ten minste een actief is. Dit systeem zorgt ervoor dat geplande en ongeplande storingen geen invloed hebben op de operatie. Dit ‘always on’-concept heeft een aantal eigenschappen die belangrijk zijn voor IGO. Met een dergelijke backbone kan Defensie:

- Veilig en federatief samenwerken. Dit is mogelijk door de goede netwerkinrichting inclusief HGI/LGI-koppeling. Denk hierbij ook aan Federated Mission Network (FMN) en Protected Core Network (PCN).
- Apparaat onafhankelijk met iedereen communiceren. De infrastructuur ondersteunt elk type device (smartphone, tablet, laptop, desktop) van elke leverancier. Daardoor kunnen gebruikers informatie daadwerkelijk altijd en overal raadplegen.
- Altijd en overal mobiele toegang bieden tot IT. Het netwerk is geen beperkende factor meer voor toegang tot IT-middelen. Er zijn wel keuzes te maken op het vlak van ontwerp en implementatie: hoe robuust en kostenefficiënt moet de infrastructuur worden?
- Elke applicatie draaien. In de toekomst zullen steeds meer applicaties voldoen aan zogenaamde ‘cloud native’-ontwikkelcriteria, waardoor ze minder afhankelijk zijn van de onderliggende cloudinfrastructuur. Dat maakt ze eenvoudig aan te passen en te migreren. Voor bestaande applicaties geldt dit niet, of in mindere mate. Deze zijn vaak meer afhankelijk van de onderliggende infrastructuur en minder makkelijk aan aanpasbaar: u kunt ze niet veranderen zonder ook de infrastructuur aan te passen. De IGO-applicaties kunnen beide zijn, of een combinatie van de twee soorten. Daarom moet de IT-backbone beide applicaties ondersteunen.

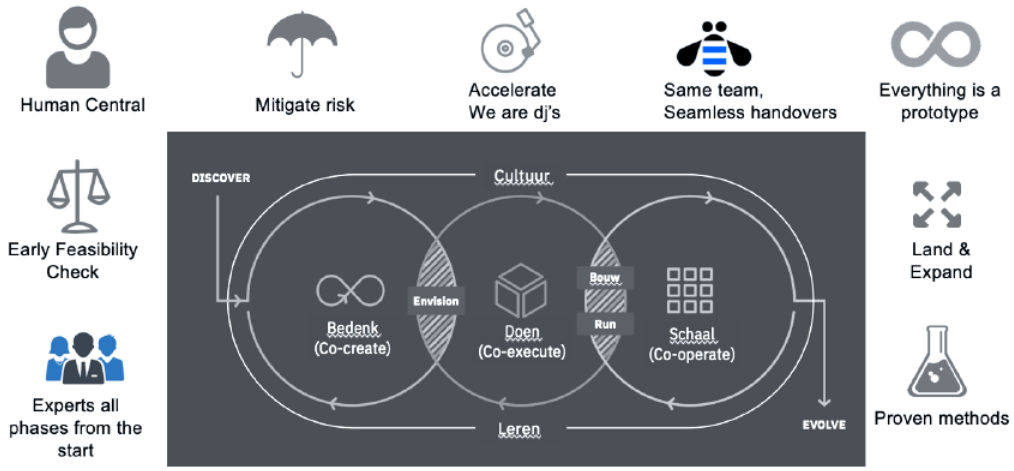
Bijlage 2

De IBM Garage Methode: de motor van een succesvolle transformatie

Vergroot de adoptie van nieuwe applicaties door een snelle ontwikkelcyclus waarbij alle stakeholders zijn betrokken

Ook grote bedrijven zijn ooit klein begonnen. Vooral de zogenaamde ‘garage startups’. Hun methode is een bekende aanpak voor techbedrijven. Ook enkele multinationals begonnen ooit in een kleine garage. IBM heeft hun aanpak gestript om de onderdelen in een roadmap te kunnen verduidelijken. Deze IBM Garage Methode biedt handvatten voor een succesvolle IGO-transformatie en sluit aan bij het besturingsmodel van Defensie zoals in **uitdaging 3** beschreven.

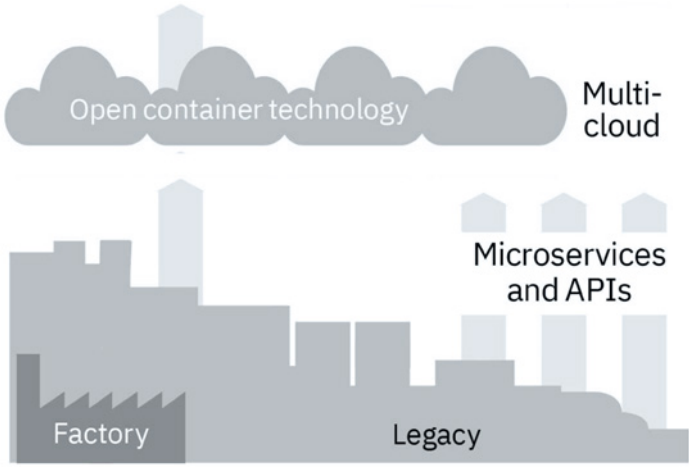
De IBM Garage Methode omvat het creëren van multidisciplinaire, cross-defensie werkruimtes. Dit zijn digitale omgevingen waar mensen uit alle lagen van de organisatie, uit diverse specialisaties, informatie kunnen delen en samen aan projecten kunnen werken. Deze cross-functionele teams kunnen hier ook samenwerken met strategische partners, zoals IBM en andere strategische en relevante partners in het defensie-ecosysteem. Hierin kunnen alle betrokkenen samen het hele proces van co-create, co-execute en co-operate doorlopen en nieuwe organisatie-platforms ontwikkelen.



IBM Garage Methode: Bedenk (Co-create), Doen (Co-execute) en Schaal (Co-operate)

Garage-omgevingen brengen innovatie op gang. Hoe? Doordat technologische opties altijd in de context van de eindgebruiker te zien zijn. De Garage Methode toetst ideeën vroegtijdig aan feedback van eindgebruikers en medewerkers. Zo voorkomt u dat tijd en budget verspild wordt. Design-thinking, agile en DevOps-benaderingen zorgen ervoor dat concepten snel worden vertaald van ideeën naar de dagelijkse praktijk. Scrums, squads en sprints helpen u om het ontwikkelproces op te delen in beheersbare, waardevolle bouwstenen. Zo kunt u met de Garage Methode snel, nieuwe organisatie-platforms ontwikkelen met een relatief laag risico. En dat opent de weg naar een continu lerende organisatie.

Garage-omgevingen sluiten aan op de factory approach van oudere (legacy) omgevingen. Dat maakt het mogelijk om nieuwe componenten te bouwen en legacy-systemen te migreren naar hybride multicloud-omgevingen en andere nieuwe platforms .



Hybride multicloud-omgevingen en Garage Methoden maken een gesynchroniseerde overgang naar IGO mogelijk

Bijlage 3

Gegevensmanagement: het creëren van een IGO-platform

Alle benodigde, actuele informatie voor iedereen real-time beschikbaar

Met een IGO-platform beschikken gebruikers over een aantal functies die helpen bij het volbrengen van hun doelstellingen. Een voorbeeld hiervan is een platform dat gebruikt wordt bij het uitvoeren van een missie. Een dergelijk platform moet diverse eenheden en strategisch partners voorzien van actuele informatie, waar ze op dat moment behoefte aan hebben. Om deze te bouwen, moet u eerst enkele zaken op een rijtje zetten. Bijvoorbeeld welke informatie getoond moet worden, welke bewerkingen er nodig zijn om tot die informatie te komen, waar de data vandaan moet komen en hoe deze data eenduidig kan worden gedefinieerd. Kortom, een breed scala aan elementen die uiteindelijk bijdragen aan het gewenste IGO-platform.

De Garage Methode kan helpen bij het realiseren van een IGO-platform. Om een goed functionerend platform te bouwen, moeten er wel op verschillende vlakken ontwikkelingen plaatsvinden. We hebben de belangrijkste hiervan, inclusief de bijbehorende aandachtsgebieden, voor u op een rijtje gezet:

Gegevensmanagement

Eenduidige gegevensdefinities en transparantie over de herkomst van gegevens waarmee de diverse krijgsmachtonderdelen snel informatie kunnen delen

Het platform moet een fundament bieden voor een aantal basisservices op het gebied van gegevensmanagement en infrastructuurfunctionaliteit. Dit vormt de basis voor de optimale synergie tussen gegevens, ontwikkeling en infrastructuur. Om het platform breed inzetbaar te maken binnen Defensie, moeten op het gebied van gegevensmanagement de volgende functionaliteiten ingevuld zijn:

- Eenduidige definitie van gegevens. Daarmee weet u zeker dat iedereen dezelfde betekenis geeft aan een gegevensobject.
- Kwaliteit van gegevens. Zo zorgt u ervoor dat de gegevens tot op een bepaald niveau juist zijn of een kwaliteitsaanduiding bieden voor gegevensobjecten.
- Classificatie van gegevens. Gegevensobjecten moeten de juiste rubricering hebben. Dat is cruciaal in de context van Defensie.
- Toegankelijkheid en eigenaarschap. Wie mag bij welke gegevens komen en door wie wordt dat bepaald?
- Regels voor anonimiseren/pseudonimiseren van gegevens. Met het oog op de privacywetgeving is het nodig om voor sommige processen gegevens te pseudonimiseren of zelfs te anonimiseren.
- Gegevens lineage (Wiv/AVG). Hierdoor kunt u achterhalen op basis van welke informatie bepaalde conclusies zijn getrokken.

Vormgeven van het integratiekoppelvlak

Eenduidige integratieservices voor applicaties, om op een veilige manier gegevens te ontvangen, verwerken en verspreiden

IGO-applicaties gebruiken standaard integratieservices van het IGO-platform. Deze noemen we Enterprise Integration Services (EIS) en een information gateway. Deze services worden aangeboden in de vorm van API's die de IGO-applicaties gebruiken om volgens standaarden informatie te delen binnen de applicatie en tussen applicaties. Deze services zorgen er ook voor dat de informatie-uitwisseling always-on is.

Selectie van nieuwe technologieën:

Met de hierboven beschreven aanpak op het vlak van gegevensmanagement en integratie, hebben we de technologische randvoorwaarden voor het bouwen van een IGO-platform geschapen. We kunnen nu diverse technologieën toepassen om de benodigde businessplatformen te creëren. Maar hoe zorgen we dat u juist die informatie kunt verwerken die van belang is, voor een of meer platformen? Daarvoor kunnen we uiteenlopende technologieën gebruiken – bestaande en toekomstige. Bijvoorbeeld een Augmented Intelligence Capability. Deze functionaliteit maakt het mogelijk om diverse oplossingen toe te passen, onder de voorwaarde dat ze middels de EIS kunnen worden aangesloten.

Daarnaast dienen de nieuwe technologieën te voldoen aan de volgende twee principes:

- **Gebruiker centraal.** Het platform moet specifieke gegevensanalyseapplicaties kunnen hosten. Bijvoorbeeld applicaties die data op een bepaalde manier verrijken en/of presenteren, met als doel de vraag van de eindgebruiker te beantwoorden. Deze tooling moet bovendien de verschillende gebruikersgroepen helpen om hun werkwijze continu te kunnen verbeteren.

- **Schaalbaar en flexibel.** Defensie moet een capability evolutionair kunnen ontwikkelen. Dat wil zeggen dat een applicatie moet kunnen doorgroeien, qua functionaliteit en capaciteit. Daardoor nemen ook de mogelijkheden van het IGO-platform toe. Zo kunnen ontwikkelde IGO-assets voor meer doeleinden binnen de krijgsmachtonderdelen gebruikt worden. Helemaal wanneer diverse gebruikersgroepen het platform kunnen uitbreiden met specifieke functionaliteit.

Meer weten over IGO Point of View?

Neem contact op met uw IBM-vertegenwoordiger

Mark Ostendorf
Client Executive Defense & Intelligence
Email: mark.ostendorf@ibm.com
Tel: +31 6 2573 2090

Edwin van der Burg
Client Technical Advisor
Email: edwinvdb@nl.ibm.com
Tel: +31 6 2255 5748

Download ook http://ibm.biz/DefensieIGO



© Copyright IBM Corporation 2020
IBM Nederland B.V.
Johan Huizingalaan 765
1066 VH Amsterdam

Produced in The Netherlands -09-2020

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at ibm.com/legal/copytrade.shtml.

Other product, company or service names may be trademarks or service marks of others. This document is current as of the initial date of publication and may be changed by IBM at any time. Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

00-NLNL-00