ROBOTICA & COMMUNICATIE

Toenemend belang van datacommunicatie op tactisch niveau

Jean-Pierre Schouwenaars, CLAS/OTCO/ LWC/CD_EGP

De operationele omgeving waarbinnen de krijgsmacht opereert verandert voortdurend. Technologische ontwikkelingen die zich snel opvolgen en elkaar versterken vereisen dat de landmacht zich continu aanpast. De visie 'Veiligheid is vooruitzien' beschrijft dit ondubbelzinnig.
De invloed van informatietechnologie, de toenemende inter-connectiviteit, verdergaande ontwikkeling van robotisering en kunstmatige intelligentie zijn van groot belang voor de krijgsmacht en de landmacht in het bijzonder. Daarom heeft Commandant Landstrijdkrachten (C-LAS) besloten een experimentele Robot en Autonome Systemen (RAS)-eenheid op te richten die is ingedeeld bij 13 Lichte Brigade. Hiermee kan stapsgewijs een capaciteit ontwikkeld worden die van grote meerwaarde is voor het toekomstig landoptreden. Wij willen winnen op het slagveld. Om dit te realiseren staat in de visie van Commandant Landstrijdkrachten dat we moeten inzetten op de verbinding tussen mens, technologie en nieuwe operationele concepten (foto 1). ➔

Foto 1, eerste stap in man-machine samenwerking: load carrying

'De mens voert het gevecht, de technologie vermenigvuldigt de gevechtskracht en met operationele concepten wordt dat gevecht georganiseerd.'
De omgeving waarin we opereren is veranderd. In die omgeving is sprake van actoren die gebruikmaken van moderne technieken waaronder onbemande systemen en intelligente sensoren. Als reactie hierop moeten we onze dominantie op het slagveld behouden en versterken, daarbij gebruikmakend van bestaande technieken en toekomstige technologische ontwikkelingen. We vergroten zo ook de veiligheid van onze mensen met de inzet van onbemande slimme systemen.

Foto 2: Themis met Remote Controlled Weapon System tijdens schietoefening in Litouwen.

Dit kan onder meer door onze *situational awareness* en slagkracht te vergroten. Daarom wordt onderzocht hoe we kunstmatige intelligentie kunnen gebruiken om de informatie van sensoren te vertalen naar de meest efficiënte inzet van onze semi-autonome systemen.
Omdat onze missies worden uitgevoerd in opdracht van de politieke leiding, is het van belang dat politieke, juridische en ethische overwegingen meegenomen worden in de besluitvorming. Het is daarom dat uiteindelijk de mens bepaalt of de inzet van semi-autonome systemen verantwoord is.

RAS-eenheid

RAS voert experimenten uit die voortkomen uit conceptueel denken. De experimenten zijn in de basis niet gebaseerd op bestaande autonome voertuigen. Dit stelt RAS in staat om met verschillende systemen te experimenteren en gecalculeerde risico's te aanvaarden. Aan de basis van deze eenheid ligt een helder geformuleerd mandaat: kennis opbouwen om uiteindelijk semi-autonome gerobotiseerde systemen operationeel in te zetten waarbij deze bijdragen aan een toename van de gevechtskracht zonder toename van benodigde mensen.
Inmiddels is al veel ervaring opgedaan. Zo zijn onbemande grondvoertuigen ingezet tijdens een (berg-) oefening in Schotland, een schietoefening in Oostenrijk en het optreden in verstedelijkt gebied in de Marnewaard.
Momenteel zijn vier bewapende systemen als operationeel experiment onderdeel van de *enhanced Force Presence* in Litouwen (foto 2). Dit is de eerste keer dat dergelijke systemen in een operationeel relevante omgeving zijn ingezet, niet alleen voor Nederland een mijlpaal maar ook binnen de NAVO.

Foto 3: de volledig elektrische Mission Master

Samenwerking

Met Nederland als kenniseconomie beschikken we over hoogwaardige technologie, intellectueel kapitaal en het vermogen om mens, technologie en innovatie samen te voegen. De RAS-eenheid wil dit kapitaal verbinden aan de behoefte van de landmacht.

Hierbij is kennis opbouwen rond mens-machine *teaming* een centraal thema waarbij de vraag is hoe mens en machine zich in de nabije toekomst tot elkaar gaan verhouden. Door een tweewegcommunicatie op te zetten tussen technische bedrijven en kennisinstellingen enerzijds en aan de andere kant een operationele eenheid, beschikken we over een unieke proeftuin waarin wij kunnen innoveren en experimenteren.

Daarom zijn partnerschappen aangegaan met civiele bedrijven en kennisinstellingen. Voorbeelden zijn samenwerkingen met *Brainport Eindhoven* via de *Safety&-Security Campus* en Milrem Robotics in Estland. Ook zijn er vanuit *Defensity College* studenten namens de landmacht bezig met het ontwikkelen van sensoren en kunstmatige intelligentie.

De RAS-eenheid heeft inmiddels ook contact met onze internationale partners, o.a. met de Verenigde Staten en Groot-Brittannië. Ondanks dat we sinds kort bestaan hebben we grote stappen gezet. Dit wordt internationaal bevestigd en daar zijn we trots op. Door onze durf om te innoveren en experimenteren doen we internationaal mee. Samenwerken is cruciaal om verder te kunnen ontwikkelen. Daarom werkt RAS gericht samen met andere NAVO landen en verkennen we een Europees platform waarin landen gezamenlijk stappen kunnen zetten om zo onze positie te versterken.

Naast deze samenwerking is er ook de samenwerking met 13 Lichte Brigade. Uit de brigade is een peloton geselecteerd dat is opgeleid op alle systemen van RAS. De onbemande grondvoertuigen zijn uitgerust met wapensystemen en we testen netwerken die drones en sensoren efficiënter data laten distribueren onder meerdere gebruikers. Dit peloton test deze middelen in realistische praktijkscenario's. Daarnaast beschikt de RAS-eenheid over een enkele *Mission Master* van Rheinmetall (foto 3).

Data, data en nog meer data

Uit alle experimenten die we tot nu toe uitgevoerd hebben, blijkt dat communicatie en datacommunicatie essentieel zijn en steeds belangrijker zullen worden. Het kunnen versturen van data in grote hoeveelheden zal moeten zorgen voor een optimaal gebruik van robots en het verzamelen, analyseren en distribueren van data. De middelen die momenteel in gebruik zijn bij CLAS zijn hiervoor niet geschikt. Daarom zijn er andere middelen aangeschaft en zijn er projecten opgestart om in de toekomstige behoefte op dit gebied te voorzien.

Om te voorzien in kritieke *command, control, communications*, *computers & intelligence* (C4I) randvoorwaarden is er besloten de MPU5 radio van *Persistent Systems* aan te schaffen. Deze van Android-OS voorziene *mobile ad-hoc network* (MANET) *software defined radio*, garandeert een robuust netwerk en biedt ook uitgebreide mogelijkheden voor breedbandige datadistributie. Optreden met robots en autonome systemen vereist veel datacommunicatie en het gebruik van sensorinformatie. Te denken valt aan data van de voertuigcamera's, *forward observer* (FO) camera's, geluidsdetectie (CASTLE), sensoren gekoppeld aan wapensystemen, *cursor on target* data al dan niet gekoppeld aan *blue force tracking* etc). De door MPU5 gebruikte 3x3 *Multiple In Multiple Out* (MIMO) technologie accommodeert dit alles. Door de combinatie van drie antennes en *multi-path* propagatie zorgt het MIMO principe voor het behalen van een groter bereik, hogere *throughput* in onoverzichtelijk, geaccidenteerd terrein of verstedelijkt gebied. Zo is een *throughput* tot 100 Mbps met de non ITAR MPU5 mogelijk.

Golfvormen en frequentiebanden

WaveRelay is de door MPU5 gebruikte *waveform*. Deze is zelf ontwikkeld door Persistent Systems, is *self healing* en is onafhankelijk van de gekozen frequentieband. Wisselen van band is eenvoudig omdat de MPU5 een modulair systeem is. Zo zijn de L/S/C-band als verwisselbare module beschikbaar. Een andere optie is het gebruik van de GVR5, de dubbelband versie. Verschillende technische mogelijkheden worden zo mogelijk voor RAS. Het terrein waarin geopereerd wordt, is bepalend voor de keuze van frequenties. Het penetratievermogen van de L-band is bijv. hoger en ook het bereik is groter. De *throughput* is daarentegen lager. Bij gebruik van de S-band en de C-band worden de bereikte afstanden kleiner maar de *throughput* hoger. Ook niet onbelangrijk is te vermelden dat er in

Foto 4: een tethered drone op een THeMIS

bepaalde landen beperkingen gelden v.w.b. het gebruik van bepaalde banden. Zo staat bijv. Duitsland niet toe dat de S-band gebruikt wordt.
Diverse banden zijn beproefd door de RAS-eenheid. Intussen is de ervaring dat een *throughput* van minimaal 20 tot 30 Mbps vereist is om adequaat met RAS-middelen te kunnen werken, dit gezien de hoeveelheid data. Het software *defined* karakter van de MPU5 staat diverse vermogens toe (0.5-10 W) maar ook verschillende frequentiebandbreedtes (5, 10, 20 Mhz). E.e.a. maakt efficiënt gebruik van de voor defensie beschikbare bandbreedtes mogelijk. Deze is immers schaars, zeker in vredestijd. De door Persistent Systems gebruikte Radio over IP (RoIP)-interface staat het tetheren toe van de MPU5 aan (*legacy*) tactische radio's. Ook dit draagt bij aan een stukje flexibiliteit.

Tethered drone

Om *line of sight* middels MANET meer bereik mogelijk te maken heeft de RAS eenheid ook de integratie van tethered drone technologie geïntroduceerd (foto 4). Door zo'n stationair vliegend systeem dat opereert tot 120 meter hoogte te koppelen aan een *unmanned ground vehicle* ontstaat een RF-paraplu. E.e.a. is tevens gekoppeld aan een adhoc routerbox die voor *beyond line of sight* (BLOS) oplossingen ook naar de MPU5 leidt. Ook beschikt deze drone over een eigen elektro-optische/infrarood (EO/IR) sensor (STANAG 4609 compliant) waarmee de *situational awareness* verder vergroot wordt.

Het verzenden van spraak en data inclusief HD-video is met de MPU5 mogelijk. Belangrijk hierbij is om te vermelden dat de traditionele spraak belangrijk blijft. Immers, de UGV treedt op als node binnen een mesh-network en kan daarmee als relay fungeren van operator naar operator, uitgestegen personeel, voertuigpersoneel etc. De meerkanaals, full duplex karakteristieken van de MPU5 staan gelijktijdige spraaksessies in meerdere gebruikersgroepen toe. Zonder encryptie kan de MPU5 niet functioneren. Daarom is ook *over the air rekeying* (OTAR) mogelijk. Hetzelfde geldt voor het laden van frequenties, *user groups* etc.

Beyond line of sight

Om *beyond line of sight* (BLOS) verbindingen te garanderen biedt de MPU5 *CloudRelay* (foto 5). Ook dit wordt intussen door de RAS-eenheid gehanteerd. Voor *CloudRelay* wordt gebruik gemaakt van een derde partij (SATCOM incl. Starlink of 4G/LTE-A/5G). Over deze middelen worden VPN IPSec-tunnels gebouwd naar het servercompartiment waar diverse services draaien. Te denken valt aan Haivision's Media Gateway, TAKServer etc.
Dit laatste staat het gebruik van *Android Tactical Assault Kit* (ATAK), WinTAK (Win voor Windows) toe voor diverse (eind)gebruikers. ATAK biedt een chatfunctie, eigen spraak, maar is in zijn algemeenheid een middel om een sterk verbeterde *situational awareness* te verkrijgen. Hiertoe zijn eindgebruikers uitgerust met zogenaamde *end user devices* (smartphone gelijkend). Voor de daadwerkelijke besturing van de THeMIS UGV wordt gebruik gemaakt van hardware (controller) en software van Milrem zelf.
De *WaveRelay waveform* van de MPU5 radio beschikt over zogeheten *Interference Resilience & Defense* (IRD). Dit is bedoeld om een robuust netwerk te garanderen dat opgewassen is tegen interferentie, bijv. door elektronische oorlogvoering. E.e.a. voorkomt het nemen van andere, drastische maatregelen zoals het veranderen van frequentie. Dat doet namelijk afbreuk aan de werking van de radio. IRD draait om een *software based library*

Foto 5: MPU 5 radio kit

met *electronic protection* maatregelen en is dusdanig geavanceerd dat het geen afbreuk doet aan de technische mogelijkheden van de radio v.w.b. schaalbaarheid, MANET *capability* etc. Zo worden connectiviteit en de diverse RF-functies gegarandeerd onder *Denied, Disrupted, Intermittent & Limited Bandwidth* (DDIL) omstandigheden. Ook kan de *library* onbeperkt worden geactualiseerd. IRD draagt zo bij aan een stukje toekomstbestendigheid.

Electronic Reconnaissance en Data-fusion & analysis

Naast de optische sensor aan boord van de *tethered drone* zoals gemonteerd op de carrierversie, is een aantal TheMIS UGVs in een *forward observer* configuratie uitgerust met bijbehorende FO-camera (EO/IR). *Full motion* videomateriaal en metadata (KLV) gegenereerd door beide sensoren wordt v.w.b. encoding, transcoding en decoding afgehandeld door de Kraken encoder aan boord van de TheMIS, de media gateway gekoppeld aan het servercompartiment. Beide producten komen van Haivision. E.e.a. maakt gebruik van Haivision's *Secure Reliable Transport* (SRT) protocol, een *data transfer protocol* gebaseerd op UDP met eigen encryptie. Dit alles zorgt voor *low latency* video zonder kwaliteitsverlies. Data van de FO camera, CASTLE, *tethered drone payload* wordt gefuseerd tot een integraal beeld in de TAK-server in het servercompartiment en vervolgens via ATAK (foto 6), WinTAK beschikbaar gesteld. Echter, als het gaat om het besturen van de UGV krijgt de desbetreffende operator direct via de MPU5 beeldmateriaal binnen van de voertuigcamera's en dergelijke.

De sensoriek wordt zoals gezegd niet alleen maar voor de besturing van systemen gebruikt, een mogelijk nog belangrijker aspect is het creëren van een objectieve en accurate *situational awareness*. Om dat te kunnen doen wordt momenteel door de RAS het eRecon en *Data Fusion Cell* (DFC)-concept ontwikkeld (foto 7). In aanvulling op de vier bewapende robots, worden er twee uitgerust met een eRecon box. Deze box bestaat uit een aantal sensoren die met name bedoeld zijn om de SA te verbeteren. De data van de sensoren van de eRecon box (akoestisch, optisch, elektromagnetisch) worden rechtstreeks naar de DFC gezonden. Zodoende kan snel en adequaat het SA-beeld gecreëerd worden. Binnen de DFC zal de analyse van de data, al dan niet geautomatiseerd, plaatsvinden. De output van de DFC zal onder andere bestaan uit opdrachten aan geautomatiseerde systemen, berichten aan eenheden voor bijvoorbeeld alarmering, berichten aan commandanten en berichten met informatie die in het commandovoeringproces opgenomen worden.

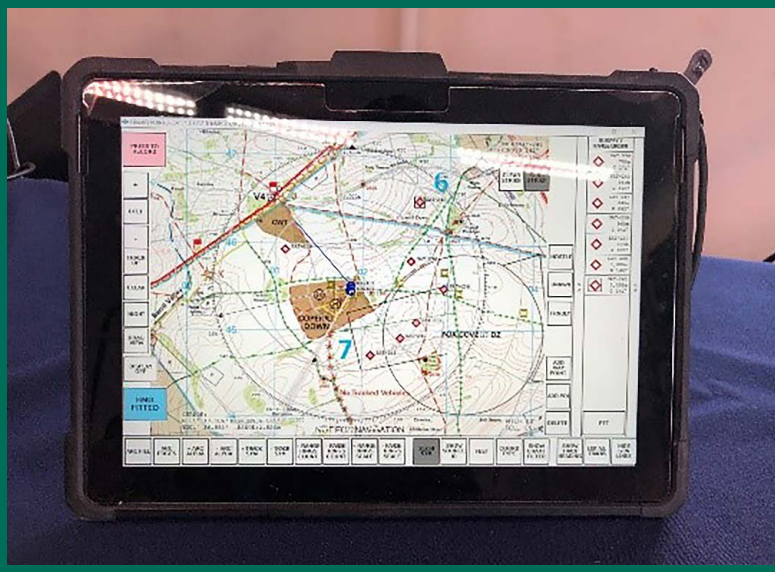


Foto 6: ATAK systeem zoals momenteel in gebruik bij RAS

Foto 7: sneak preview van de DFC (in aanbouw) zoals die tijdens de experimenten van 2023 ingezet gaat worden

Ing. M. de Wit- Blok

GEEN DATA...

GEEN INFORMATIEGESTUURD OPTREDEN!

In de DefensieVisie 2035 staan nieuwe technologieën op een prominente plaats. Deze technologieën zijn onder meer nodig om een invulling te kunnen geven aan IGO – Informatiegestuurd Optreden. Hieronder ook technologieën voor de opslag en het beheer van data. Want hoe zorg je ervoor dat de 'mega' grote hoeveelheden gegevens efficiënt en veilig zijn op te slaan en zodanig dat ze realtime zijn te analyseren en te ontsluiten voor de hele krijgsmacht? Dyon Dohmen en Chris Vardaris vertellen welke rol dataopslag en -managementsystemen van NetApp nu al spelen bij de Nederlandse Defensie en wat we in de toekomst kunnen verwachten.

Missies uitvoeren is een gevecht geworden om de beste informatiepositie. De partij die het snelst over de meeste relevante kennis kan beschikken – gebaseerd op de verzameling van data en de omzetting ervan in informatie – heeft een voorsprong. Zowel militairen op de hightech commandocentra áls de militairen in het veld. Wat dat betreft is de zogenaamde informatiedominantie een geducht wapen in de strijd tegen vijandelijke facties geworden.

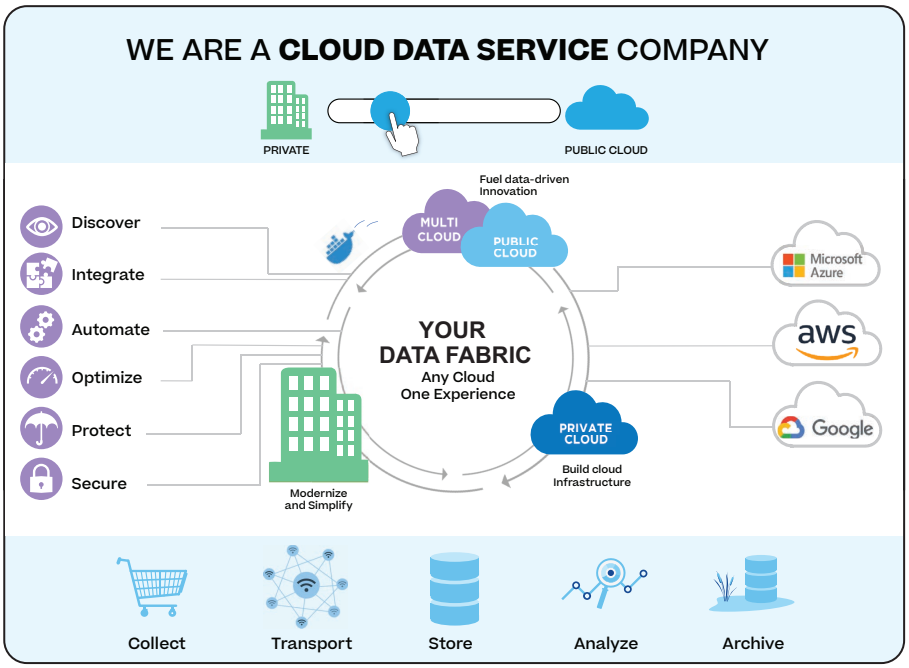
Nu leven we gelukkig in een tijd waarin het verzamelen van data relatief eenvoudig is geworden. Sensoren en meetapparatuur zijn relatief goedkoop geworden, een veilige verzending naar een centraal punt is geen probleem en de rekencapaciteit van computers is dermate groot dat de analyse van data voor niet al te grote hoeveelheden tegelijk bijna realtime mogelijk is. Deze mogelijkheden stellen ons echter ook weer voor nieuwe uitdagingen.

Een relatief bekende quote van voormalig CDS Rob Bauer tijdens de presentatie van de DefensieVisie 2035 luidt: "Vroeger hadden we altijd te weinig inlichtingen, nu hebben we zoveel data dat we erin verzuipen als je niet uitkijkt." Zijn uitspraak verwijst haarfijn naar de cruciale stap die moet worden gemaakt om van de juiste data de juiste informatie te maken en dat het liefst zo snel mogelijk. Uiteraard met het doel deze informatie vervolgens beschikbaar te hebben op het juiste tijdstip, op de juiste locatie (land, zee of lucht) en uiteraard bij de juiste persoon.

Opslag en beheer

"Om dit technisch te realiseren zijn geavanceerde maar ook slimme systemen nodig. Het gaat immers over IT, over opslag, over zoeken maar ook over de juiste locatie waar data wordt opgeslagen in het kader van vindbaarheid", meent Dyon Dohmen.

Dohmen is Senior Client Executive bij NetApp, een van oorsprong Amerikaans bedrijf dat dertig jaar geleden werd opgericht in Silicon Valley. Hier is de afgelopen drie decennia een schat aan kennis en ervaring ontwikkeld op het vlak van dataopslag en -managementsystemen. Daarbij is indertijd de keuze gemaakt om gebruik te maken van standaard hardware en de applicatie door middel van geavanceerde software klantspecifiek maken. Hij vervolgt: “Alleen partijen die in staat zijn deze hoeveelheid gegevens compact op te slaan en te beheren, voldoen aan twee belangrijke randvoorwaarden van IGO. Met beheren bedoelen we dan: snel de juiste informatie kunnen vinden en ontsluiten maar ook up to date houden, back-uppen, borgen, verplaatsen of verwijderen wanneer dat nodig is.”



Data Fabric

Data Fabric

De basis voor de applicaties die NetApp inmiddels voor vele (grote) partijen ontwikkelde, is de datamanagementsoftware ONTAP.

Voorbeeld dataopslag in ‘laag 3’

Het Amerikaanse Department of Defense gebruikt voor haar speciale eenheden (special operations forces), de technologie van NetApp om data te repliceren. Zowel binnen de Verenigde Staten als daarbuiten. Hiermee wordt een zogenaamd wereldwijd Datameer gecreëerd waarvan alle bevoegde mensen gebruik kunnen maken. In het kader van veiligheid worden op missie alle bestanden die niet binnen 30 dagen worden aangeraakt, automatisch door de software naar de zogenaamde S3 opslaglaag gebracht. De gebruiker ziet en merkt hier niets van, maar het kost uiteindelijk wel minder ruimte. Wanneer het bestand nodig is, haalt de software het bestand terug van het dichtstbijzijnde S3-knooppunt en begint de 30-daagse timer opnieuw. Uiteindelijk is er op missies op deze manier een kleiner databestand aan te houden.

Via deze software is de opslag van data flexibel te implementeren in verschillende architecturen; variërend van hardware opslagsystemen, software-defined storage (SDS) of de cloud. NetApp ontwikkelde tevens een eigen data architectuur in de vorm van Data Fabric. Deze architectuur zorgt voor de samenhang tussen opslagsystemen, regelsystemen (software) en Cloud dataservices. In bovenstaande figuur is schematisch weergegeven uit welke elementen deze architectuur bestaat en wat hun specifieke rol is.

Centraal staat de ‘data fabric’ oftewel: de organisatie die data genereert. In dit geval alle mensen en technische installaties, voertuigen en apparaten van Defensie en relevante partners. Dit kunnen enerzijds geclassificeerde data zijn maar tevens openbaar toegankelijke informatie zoals een routeplanner, de weersverwachting of de luchtkwaliteit. Aan de onderkant van het schema is weergegeven wat er met de data gebeurt: deze wordt verzameld, getransporteerd, opgeslagen, geanalyseerd en vervolgens gearchiveerd voor gebruik. Voor al deze processen, van het verzamelen tot het archiveren, heeft NetApp oplossingen ontwikkeld die bijdragen aan onder meer efficiëntie, veiligheid en de mogelijkheid tot dynamisch gebruik en automatisering. Enkele van deze punten zijn te vinden aan de linkerkant van de tekening. Aan de rechterzijde zijn enkele grote partijen te zien waarmee de data fabric in verbinding staat en waarvan de services direct beschikbaar zijn.

Chris Vardaris is Solutions Engineer bij NetApp en geeft aan: “Het voert te ver om alle eigenschappen van ONTAP en de Data Fabric hier te benoemen. Deze variëren van het eenvoudig back-uppen van data tot aan beveiliging tegen bijvoorbeeld cyber security (zie ook kaders). In het kader van een gebruiker als Defensie wil ik echter graag de mogelijkheden voor opslag apart benoemen. In het bedrijfsleven en de industrie speelt opslag in de cloud een

steeds belangrijker rol. Om veiligheidsredenen maakt Defensie praktisch geen gebruik van de publieke cloud maar richt zich meer op het gebruik van zogenaamde secure cloud providers. Dit is een oplossing waarbij Defensie wel gebruik kan maken van de (reken)capaciteit van de grote cloud providers zónder dat hiervoor het publieke internet wordt ingezet.

Naast veiligheid van opslag speelt ook efficiëntie een belangrijke rol. De hoeveelheid gegevens die dagelijks binnen Defensie wordt gegenereerd is dermate groot dat je hier niet afkunt met een soort externe harde schijf of extra server. Defensie is overigens niet de enige organisatie die hiermee te maken heeft en de afgelopen jaren zijn er door NetApp dan ook verschillende slimme oplossingen ontwikkeld waarmee data heel compact is op te slaan. Dit bespaart niet alleen in footprint maar biedt tevens de mogelijkheid om snel en vaak een backup te maken. Bovendien ondersteunt het de mogelijkheid om data snel te kunnen uitwisselen of testen."

Common Data Layer

Vanwege het bijzondere karakter van de Defensieorganisatie, is hiervoor een aparte Data Fabric ontwikkeld: de common data layer.

Chris Vardaris: "De nadruk ligt hier op veiligheid. Een structuur die veilig is in te vullen en te gebruiken. Zoals in onderstaande afbeelding te zien, is data in uiteenlopende typen informatiesystemen en applicaties te genereren en – wanneer zij met elkaar zijn verbonden – eenvoudig onderling uit te wisselen. Omdat dit binnen de Common Layer op een uniforme en open manier gebeurt, is het ook mogelijk om de data veilig over de verschillende domeinen te verplaatsen."

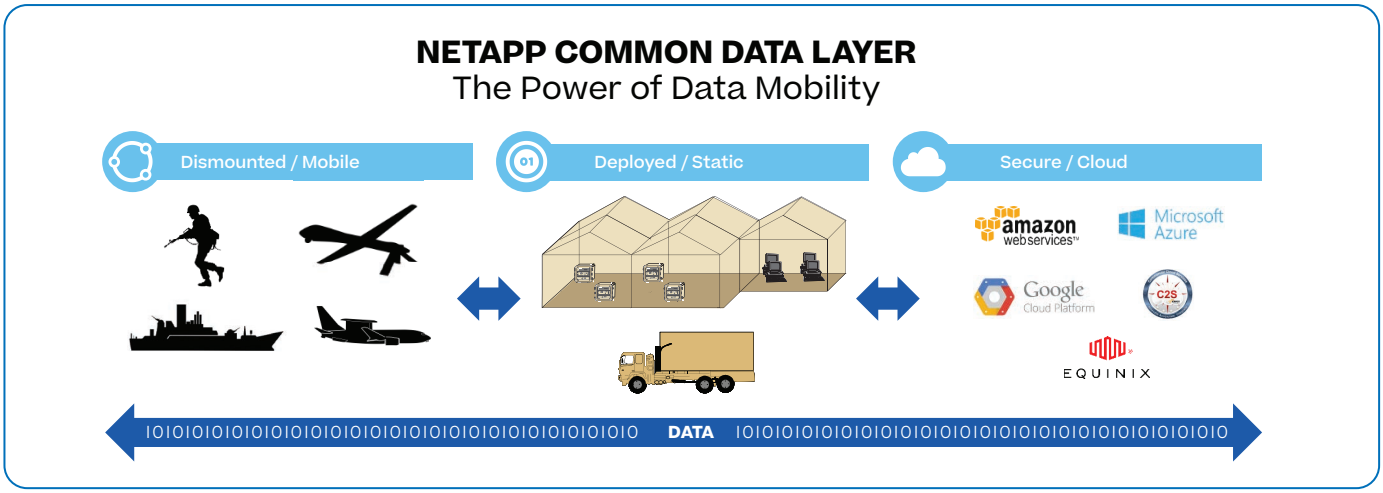
Aan de linkerkant het mobiele domein waarin militairen daadwerkelijk in het veld opereren en voor het succes van hun optreden deels afhankelijk zijn van de beschikbare informatie. Voor dit domein is het belangrijk dat de oplossingen robuust zijn en dat veel data compact is op te slaan. Tevens biedt het voordelen wanneer data op een slimme manier zijn te verplaatsen zonder menselijke interactie. Van actor en sensor tot datacenter. Verder ligt er een nadruk op de toepassing van radio- en satcomnetwerken met een beperkte bandbreedte.

Dyon Dohmen: "Kijken we naar de statische omgeving zoals een kazerne of commandopost, dan is dit een omgeving of domein waar data realtime direct beschikbaar is en het updaten van de informatie voortdurend kan plaatsvinden zonder downtime. Verder moeten de oplossingen snel en efficiënt werken om AI-toepassingen (artificial intelligence) mogelijk te maken. Tevens ligt hier de basis voor een combinatie van de cloud en de eigen datacentra voor het beheer van zeer grote hoeveelheden data. Dit noemen we ook wel multi-petabyte. Daarbij is een petabyte, afgekort PB, gelijk aan 1.000 terabytes ofwel 1.000.000.000.000.000 bytes (1015 B). Met dergelijke grote hoeveelheden geldt uiteraard dat er gebruik wordt gemaakt van een geïntegreerde data security en dat een hoge opslagefficiëntie en datamobiliteit van belang zijn."

Tot slot de opslagomgeving of de 'Secure Cloud' als derde domein. Hier is het hoogste niveau van beveiliging van data van toepassing. Onder meer door zeker te stellen dat toegang uitsluitend wordt verleend aan geautoriseerde personen. Bovendien is de cloud door de grootte en beschikbare rekencapaciteit bij uitstek de plek om data te analyseren om op deze manier informatie te creëren. Dit wordt ook 'near cloud data' genoemd en betekent dat de data op het eigen private systeem worden opgeslagen maar dat wel gebruik is te maken van de ruimte en capaciteit van de cloud om de data te analyseren. Chris Vardaris: "Hierin bestaat ook de mogelijkheid om data te scheiden naar behoefte en beschikbaarheid. Voor Defensie zou dit een goede oplossing kunnen zijn."

Praktische voorbeelden Common Data Layer

Welke voordelen de Common Data Layer in de praktijk biedt, blijkt uit enkele voorbeelden die NetApp uiteenzet. Als eerste is dit de 'mobiele beschikbaarheid van data'. Dyon: "De Common Data Layer maakt het mogelijk om relevante data overal beschikbaar te hebben. Zowel op het land als op het water of in de lucht. Hiervoor wordt data uniform opgeslagen wat betekent dat er



Common Data Layer

gebruik wordt gemaakt van open standaarden. Daarbij is onze data-infrastructuur zogenaamd 'software defined' wat betekent dat op- en afschalen relatief eenvoudig is.
Verder is de infrastructuur hiermee ook geschikt voor ICT-componenten met een andere vormfactor dan in het datacenter gebruikelijk is. Bijvoorbeeld componenten die bestand zijn tegen extreme omstandigheden zoals deze in het veld kunnen optreden. Denk daarbij aan hoge of juist lage temperaturen, schokbelastingen en trillingen. Met deze componenten profiteert iedere militair op iedere locatie dus van de maximale beschikbaarheid van gegevens terwijl hij de hardware – zelfs een mini datacenter – gewoon in zijn rugzak kan meenemen."

Chris Vardaris vervolgt: "Om de data die militairen ter plekke verzamelen te kunnen analyseren, bijvoorbeeld in het kader van situational awareness, is het belangrijk dat de data op een uniforme manier zijn uit te wisselen met de statische (kantoor of commandopost) omgevingen. De systemen in deze omgevingen zijn weliswaar groter, maar werken op dezelfde software en open standaarden waardoor dit mogelijk is. Ook wanneer het om uitwisseling gaat met NATO-bondgenoten die een compatibele data-infrastructuur hebben."

Bijzonder is verder de rol die AI in de applicatie speelt om de grote hoeveelheid data te verwerken die dagelijks wordt gegenereerd. Dit is onder meer mogelijk door de ontwikkelingen in de chipsector, waarbij processoren en geheugenmodules steeds kleiner worden. Dyon Dohmen: "Juist deze ontwikkelingen maken het mogelijk om AI ook in het mobiele domein toe te passen zodat operationele eenheden de informatie letterlijk in het veld beschikbaar hebben. Bovendien zijn gegevens die zij verzamelen weer snel terug te koppelen naar de centrale datacenters voor verdere verwerking."

Binnen de Nederlandse Defensie

NetApp is inmiddels op diverse plekken binnen de Nederlandse Defensie te vinden met de ONTAP datamanagementsoftware die op verschillende (virtuele) appliances draait. Dyon Dohmen "We zijn al zo'n vijftien jaar geleden met Defensie in gesprek geraakt via een technisch symposium. Dat gesprek ging in eerste instantie over de opslag van data. In die tijd werd er dagelijks een back-up gemaakt wat voor een organisatie als Defensie relatief weinig is. Dit gesprek leidde uiteindelijk tot de implementatie van een ander type opslagsysteem waarbij ieder uur een soort 'foto' wordt gemaakt van de data. Een snapshot noemen we dat. Deze snapshots zijn te maken terwijl iedereen aan het werk is en het mooie is: iedere volgende snapshot wordt vergeleken met zijn voorganger en alleen de veranderingen worden opgeslagen. Dit scheel veel tijd en ruimte maar bovenal kun je op deze manier bijna niets kwijtraken. Als er wat gebeurt, is de impact minimaal omdat je altijd je data terug kan halen vanuit een recente snapshot. Snapshots zijn standaard weliswaar 'read-only', maar kunnen ook zodanig worden ingesteld dat ze een bepaalde tijd door niemand zijn te wissen. Snapshots zijn dan ook per definitie de 'redding' als ONTAP ransomware activiteiten detecteert. Hiervoor beschikt ONTAP over een machine learning engine die 24/7 waakzaam is op ransomware aanvallen op de data die op de ONTAP systemen staan."

Hij vervolgt: "In de jaren die volgden is onze software ONTAP binnen vele andere toepassingen geïmplementeerd en daarbij gekoppeld aan onder meer SAP en MULAN. Maar er is in onze optiek nog veel meer mogelijk. Zo zie je binnen de Nederlandse Defensie nog relatief veel zogenaamde silosystemen waarbij ieder onderdeel zijn eigen silo heeft en het daar zelf regelt. Het zou veel voordelen opleveren wanneer de onderdelen werden gekoppeld en alle medewerkers kunnen putten uit dezelfde bron – de single source gedachte. Het verkleint de totale opslagbehoefte en hiermee de kosten en draagt bovendien bij aan de reductie van fouten die het gevolg zijn van informatie die op verschillende locaties in verschillende versies voorkomt. Want één ding is zeker: Waarvan er meer versies beschikbaar zijn, is er altijd meer één versie up-to-date en de rest verouderd. Verder is de schaalbaarheid vele malen groter dan bij silo's überhaupt is te realiseren. Dat betekent dat je altijd zonder problemen een applicatie kunt toevoegen maar ook weer kunt verwijderen. Uiteraard moet je dan wel kunnen werken met oplossingen die in staat zijn om grote hoeveelheden data efficiënt en veilig te managen.

Voor de toekomst is het denk ik goed om de aandacht nog wat meer naar opslag in de cloud te brengen. Door gebruik te maken van de cloud is data nog eenvoudiger op locatie te krijgen, tot aan een afzonderlijk voertuig toe, en biedt de mogelijkheid om méé te kunnen in de internationale ontwikkelingen binnen NATO. Technisch en veiligheidstechnisch is dat in deze tijd geen probleem meer. Vragen? Zie je mogelijkheden? Neem graag contact op!"

Opslag geclassificeerde informatie

In het Verenigd Koninkrijk wordt de hoger gerubriceerde informatie (HGI) op de NetApp data-infrastructuur opgeslagen. Dit gebeurt snel en efficiënt (compact formaat) op verschillende plekken in de wereld. Via het NetApp platform wordt deze data verder gedistribueerd voor onder meer analysedoeleinden waarbij de gebruiker profiteert van een snelle datadistributie zonder de noodzaak van conversie.