# 1GNC: EEN VERANDERENDE OMGEVING, INNOVATIEKANSEN

Kapitein D.P.G.L. van de Braak, Chief MCCC van het CIS Battalion van 1GNC

**Kap Dennis van de Braak is na een afwezigheid van 10 jaar terug bij Defensie en bij de Verbindingsdienst. In die 10 jaar is hij werkzaam geweest bij diverse ICT-bedrijven van technisch specialist, afdelingsmanager tot projectmanager. Ook deze ervaringen blijken bruikbaar en toepasbaar in zijn huidige functie: Chief MCCC van het CISBn van 1GNC. In dit artikel 'rekt en strekt' kap Van de Braak het gebruik en de toepassingen van TITAAN en plaatst dat tegen de praktische operationele realiteit van de oefening COLD CHALLENGE 2011. Innovatie: niet omdat het kan, maar omdat het moet.**

## INLEIDING

Vanaf mijn plaatsing in 2008 tot heden, heb ik veel ervaring opgedaan met TITAAN-4 en heb ik ook mijn civiele ervaring kunnen toepassen. Als Chief van het MCCC geef ik mede richting aan de wijze waarop wij de klant ondersteunen en is het MCCC een *key player* in dit proces.
Sinds 2007 is TITAAN versie 4 ingevoerd bij 1GNC. Na praktische ervaring opgedaan te hebben met TITAAN 4 binnen het CISBn, worden de voor- en nadelen van het systeem zichtbaar; daarnaast verandert de wereld om ons heen en stelt de klant nieuwe eisen. Welke innovatie kunnen we zelf toepassen aan TITAAN? Ik noem dit het 'rekken en strekken van TITAAN' en wil daarmee zeggen dat innovaties niet het totale concept moeten veranderen.

## INNOVATIES BINNEN 1GNC

Binnen het CISBn van 1GNC vindt er innovatie plaats waarover ik u wil informeren:
- de mogelijkheid die het internet biedt om TITAAN te verlengen;
- een alternatieve inrichting van TITAAN waarmee we de voorbereiding van het systeem, het *Prime and Stage* proces, kunnen bekorten en tot slot
- de veranderende klantbehoefte en welke oplossingen we daarop in antwoord kunnen bieden.

Per onderwerp zal ik de centrale vraag 'welke innovatie kunnen we zelf toepassen' trachten te beantwoorden door antwoord te geven op de vragen:
- welke innovatie is gewenst;
- wat is er mogelijk en
- welke innovatie daarvan kunnen we zelf toepassen.

Met dit artikel wil ik niet alleen de discussie starten waar de ontwikkeling van TITAAN heen moet, maar ook de opgedane ervaring en bijbehorende innovatie, delen. Ik besef dat dit onderwerp soms vrij diep kan ingaan op de materie. Desondanks tracht ik door de meeste begrippen te verklaren, u inzicht te geven over deze innovatieve kans.

## TITAAN VERLENGEN VIA INTERNET

**Situatie**
In de voorbereiding van de oefening COLD CHALLENGE 2011 van 1GNC werden we (het MCCC van het CISBn) geconfronteerd met de geografische beperkingen van Noorwegen. Satellietcommunicatie met de ons ter beschikking staande satellieten is daar mogelijk onder een elevatiehoek van 7 graden. Een elevatiehoek van 7 graden betekent ook dat een *line-of-sight* van 2 km nodig is. Gezien het bergachtig landschap loopt je hier al snel tegen beperkingen aan en wordt het alleen maar lastiger wanneer er ook nog begroeiing in de weg staat.

Een alternatief is het realiseren van een *point-to-point* geschakelde verbinding. De aanwezige ICT-infrastructuur bood deze mogelijkheid. Binnen TITAAN hebben we hier de verbinding gebaseerd op de LEU (*Link Encryption Unit*) als toepassing, maar geschakelde verbindingen over een behoorlijke afstand (Duitsland-Noorwegen) zijn een kostbare aangelegenheid.
Beide oplossingen bieden een WAN-verbinding die theoretisch maximaal 2 Mbps bedraagt.
In de figuur op devolgende bladzijde ziet u de geografische verspreiding van de stafelementen. Bijzonder hierin is dat het stafelement van 1GNC, dat deelneemt in de *Directing Staff* (DISTAFF) van de oefening, dezelfde informatie wil delen en bewerken als de MAIN-CP van 1GNC. Dit stafelement, voor het gemak maar even de Forward CP genoemd, bevindt zich in Evenes (Noorwegen). De MAIN-CP 1GNC bevindt zich in Münster (Duitsland).

**Welke innovatie is gewenst?**
Verschillende CP'n willen informatie kunnen delen en bewerken. In het standaard TITAAN-concept hebben CP'n een eigen, gesloten omgeving. Informatie kan gedeeld worden door dit te e-mailen (Themis of Outlook) of via een Webportaal te publiceren. Hiervoor wordt bij 1GNC het door NATO ontwikkelde WISE, *Web Information Services Environment*, gebruikt. De C-1GNC en zijn staf moesten in staat zijn om vanuit de Forward-CP op een zelfde wijze, als waren ze in de MAIN-CP aanwezig geweest, leiding te geven aan 1GNC. De totale staf zou uit 35 personen bestaan.
Er was behoefte aan een alternatief en betaalbare WAN-verbindingsmiddel. De beschikbaarheid van Satcom was onzeker en een LEU-verbinding bleek te begrotelijk.

**Wat is er mogelijk?**
Wil je de informatie gezamenlijk bewerken dan denk je al gauw aan zogenaamde online-collaboration software. Microsofts SharePoint Portal is hier een eigentijds voorbeeld van. Tijdens de oefening NEMESIS SWORD 2010 was er al een bruikbaar alternatief ontwikkeld. In deze oefening was er gelijke informatiebehoefte tussen de MAIN-CP en de EXCON-CP. De eenvoudige oplossing hierop was het maken van een zogenaamde trust-relatie tussen de CP'n. Gebruikers van de ene CP werden vertrouwd om toegelaten te worden op de andere CP. Een standaard Microsoft-oplossing tussen zogenaamde domeinen, maar niet een oplossing die slim omgaat met beperkte bandbreedte, zoals de maximale 2 Mbps in Satcom- en LEU-verbindingen. Documenten worden steeds groter en zo ook vraagt het toepassen van een trust met meerdere gebruikers dus ook om een breedbandige verbinding. In de oefening NEMESIS SWORD was dat geen beperking omdat er op glasbasis, 100 Mbps, gekoppeld werd.
Op zoek naar een alternatief voor de be-


*Geografische contouren van COLD CHALLENGE 2011*

staande WAN-verbindingsmiddelen èn op zoek naar een breedbandige oplossing bracht mij dit bij een *lead-architect* van C2SC, de heer drs. C.M. van Munster. Hij had al eerder een concept beproefd waarin een tunnel over internet werd gebouwd met behulp van de tunnelbox. Het vereist dan wel een aanpassing aan de box omdat het concept van multicasting (multicast: connectieprincipe waarin één bron communiceert met een geselecteerde groep ontvangers, door middel van één uitzending) hierin niet wordt gebruikt. Een tweede aanpassing aan de box was nodig om een hogere brandbreedte dan 2 Mbps te behalen. De versie van de crypto-apparaat, de TCE-621, is hier de beperkte factor. Door meerdere TCE'n in te bouwen en deze parallel te schakelen, kan een hogere bandbreedte bereikt worden. Een aangepaste tunnelbox kan dus een vercijferde, breedbandige tunnel opbouwen via het internet.

**Welke innovatie kunnen we zelf toepassen?**

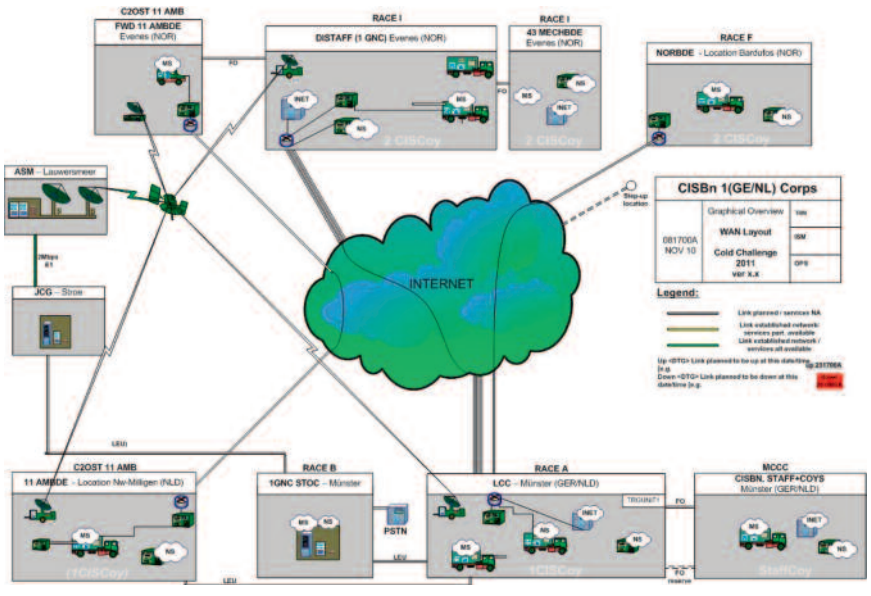
Het implementeren van *online collaboration* software is behoorlijk ingrijpend. Niet alleen is hiervoor servercapaciteit en software benodigd maar vraagt het ook om opleiding van gebruikers en beheerders. Daarnaast moeten procedures hierop aangepast worden.

Kortom in mijn overweging, te ingrijpend om zelf (als gebruiker) te implementeren en wellicht beter om dit als veranderwens in te brengen in een nieuwe versie van TITAAN. Het opzetten van een trust tussen domeinen, in TITAAN CP'n, is redelijk eenvoudig uitvoerbaar. Met een zeer beperkt aantal gebruikers hoeft dit geen consequenties te hebben voor het gebruikte WAN-middel. In het door mij geschetste scenario echter, het ontwerp voor oefening COLD CHALLENGE, kon dit alleen maar als de WAN-verbinding breedbandig zou zijn en meer dan 2 Mbps.

Het gebruik van een standaard tunnelbox met één TCE is voor dit doeleinde zelf configureerbaar terwijl een oplossing met meerdere TCE'n, en dus hogere brandbreedte, een *special* is die niet zonder de ondersteuning van de ontwikkelaar uitgevoerd moet worden. Hiertoe moet immers een tunnelbox ingrijpend aangepast worden.

Nadelen? Ja, het blijft natuurlijk een koppeling aan een onveilig netwerk. De crypto is van dien aard dat we ons daarom geen zorgen hoeven te maken, het apparaat is hiertoe ook geclassificeerd. Wel zullen we bescherming moeten toepassen tegen een breed scala van (externe) bedreigingen, waaronder de meest bekende en beruchte *(Distributed) Denial of Service* aanval.

Ter illustratie ziet u hier een WAN-ontwerp voor oefening COLD CHALLENGE 2011.




*WAN-overview COLD CHALLENGE 2011*

## BEKORTEN VAN HET PRIME AND STAGE PROCES

**Situatie**

Het primen (initiële installatie) en het stagen (configureren op de missie) van TITAAN-4 servers, is een tijdrovend proces (Prime and Stage – P&S). In het CISBn wordt voor de totale voorbereiding 3,5 week uitgetrokken: 2,5 week P&S en 1 week systeemtest. Natuurlijk zit hier een extra marge in tijd berekend, maar deze is ook vaak benodigd door allerlei oorzaken:

- bovengemiddelde defecte hardware;
- regelmatige her-installatie van Domain Controllers;
- *human factor*.

Defecte hardware wordt vooral veroorzaakt door het feit dat apparatuur langere tijd uit heeft gestaan. Deze civiele apparatuur is hier niet voor ontworpen en het wordt nog erger wanneer er ook geen opslagverwarming heeft plaatsgevonden. Een aanzienlijke hoeveelheid hardware vertoont in de eerste weken defecten en moet worden vervangen.

Domain Controllers (DC) moeten in de installatie de *Unattended Server Installation* (USI) simultaan en succesvol doorlopen. Wanneer één DC een *error* heeft, moeten alle DC's opnieuw geïnstalleerd worden. Een *fail-over* is al een tweede DC in één domein. In geval van ACP/RCP zijn er 4 DC's actief in één domein. In de praktijk gaat dit vaak fout, wat leidt tot re-USI.

De *human factor*. Een verkeerde inschatting of configuratieparameter kan verstrekkende gevolgen hebben. In de praktijk zien we dat verkeerde servers een her-installatie krijgen of dat een fout in de benaming pas na 1,5 week zichtbaar is in het systeem. Ook de configuratie van het netwerk voordat USI kan starten, reken ik hier toe. Dit netwerk

bevat initieel veel fouten die opgelost moeten worden voordat USI überhaupt kan starten. Deze netwerkcontrole is in de procedure van het CISBn toegevoegd.

**De inrichting van de servers is gebonden aan een eenheid**

Voordat het P&S-proces kan starten, moet eerst de *order of battle* (ORBAT) bekend zijn. Deze ORBAT wordt pas bekend nadat het besluitvormingsproces is beëindigd. De ORBAT echter, is een noodzakelijke parameter in de planning van een missie of oefening.

Nadat de ORBAT bekend is, zal iedere eenheid worden geconfigureerd op een eigen toegewezen server of worden ondergebracht bij een eenheid met eigen server (*hosted*). In het P&S-proces is de eerste eenheid, de zogenaamde *First unit*, uniek voor een installatie en kan later niet meer worden veranderd. Aanpassen kan dan alleen nog maar door het P&S-proces opnieuw te doorlopen. Ook additionele eenheden toevoegen aan de missie of oefening, op eigen toegewezen hardware, kan alleen door het P&S-proces opnieuw te doorlopen voor die eenheden.

**Welke innovatie is gewenst?**

Al enige tijd geleden, heeft de G6 van 1GNC aangegeven dat het P&S-proces te veel tijd kost. In geval van nationale operaties is deze voorbereiding al helemaal ongewenst. Daarnaast is de verhouding zoek bij bijvoorbeeld een bataljonsoefening van één week. Het kost dan 3,5 week voorbereiding om effectief één week te oefenen. 1GNC heeft behoefte aan flexibiliteit als het gaat om toewijzen van eenheden aan CIS-middelen. De exacte initiële ORBAT kan op voorhand nog onduidelijk zijn en daarnaast kunnen onder bevel gestelde eenheden wisselen. Alleen een flexibel CIS kan hier een antwoord op bieden.

Binnen het bataljon is er behoefte aan een CIS-omgeving voor trainingsdoeleinden. Denk hierbij aan compagniesoefeningen en activiteiten op niveau 1 tot en met 3.

**Wat is er mogelijk?**

In mijn onderzoek waarom TITAAN bij iedere oefening of missie volledig opnieuw geïnstalleerd en ingericht wordt, kwam ik erachter dat dit veiligheidtechnisch gerelateerd is. Op advies van de Beveiligingsautoriteit van de Bestuursstaf is het systeem op deze manier ontworpen. Op deze manier kan er nooit informatie van een eerdere oefening of missie aanwezig zijn en tot compromitatie of vervuiling leiden. Dit in het achterhoofd houdende, ging ik op zoek naar een oplossing en kwam tot het volgende:

- de afhankelijkheid van de ORBAT moet sterk verminderd worden;
- in het P&S-proces kan een scheiding worden aangebracht tussen missiegerelateerde data en generieke inrichting en
- wanneer het hosten van een eenheid eenvoudig toe te voegen is op een al ge-P&S'de omgeving, waarom hosten we dan niet alle eenheden?

**Uitwerking**

*Hosted unit*

De *Rapid CIS Element* (RACE) of C2 Ost element wordt de *First unit* van de server. De domeinnaam wordt gemakshalve DOMAIN F (Foxtrot of Golf, etc.) genoemd, gelijk aan de naam van het RACE (F). Alle eenheden worden als *hosted units* geconfigureerd op de server. Een *hosted unit* kan eenvoudig worden toegevoegd of zelfs worden verhuisd naar een andere server. Hier ontstaat een nieuw CIS-proces; MOVE UNIT. De afhankelijkheid van de ORBAT wordt op deze manier sterk verminderd. Scheiding van de missiegerelateerde data en de generieke inrichting van een server, wordt eenvoudiger als bovengenoemde oplossing toegepast wordt. Op een gegeven moment zullen de *hosted units* aangemaakt moeten worden. Hier ligt dan een mogelijkheid tot scheiden van deze data op de inrichting.

De ingewijden onder u zullen zeggen dat wanneer de CIS-processen zoals *Transfer of Command of Relocate* uitgevoerd worden, deze invloed hebben op dit concept. Dit klopt en daarom is het erg belangrijk om hiermee rekening te houden. Een *Transfer of Command* zal alle eenheden op die omgeving beïnvloeden en wellicht vooraf gaan door een *Unit move* van een enkele eenheid die dit niet wenst. Een ACP/RCP-constructie moet dan ook één zogenaamde *dedicated* eenheid kennen.

De voordelen:

- het P&S-proces kan starten voordat de ORBAT bekend is;
- (kleinere) eenheden kunnen eenvoudig in later stadium worden toegevoegd via de *join (hosted) unit* procedure en
- in het P&S-proces kan de situatie voordat de eenheden geladen zijn, bevroren worden. Dit saven van de situatie kan bij volgende keren tot enorme tijdbesparing leiden.

Deze laatste mogelijkheid ga ik verder toelichten.

*Saven* situatie

Iedere TITAAN-server heeft een zogenaamde RAID-1 (mirror) configuratie. Dit wil zeggen dat er twee harde schijven aanwezig zijn, gespiegeld naar elkaar. Een harde schijf uit een mirror kan eruit gehaald worden en vervangen door een nieuwe, blanco, harde schijf. Het RAID-1 systeem zal dan automatisch deze schijf weer beschrijven met exact dezelfde informatie als de andere harde schijf.

Dit biedt de mogelijkheid om één schijf uit de mirror op te slaan en te gebruiken voor toekomstige installaties. Ideaal natuurlijk wanneer dit gebeurt na het P&S-proces en voordat de eenheden toegevoegd worden. Deze uitgenomen harde schijf bevat dat een situatie die we kunnen noemen de *Starting point*. De *Starting point* harde schijf eenvoudig uitnemen en bewaren tot een volgende gelegenheid, gaat niet zo eenvoudig. Het bevat nog steeds een Microsoft server die behoefte heeft om binnen een gestelde tijd de andere servers te 'zien' en daarmee te synchroniseren. Gebeurt dit niet, dan wordt de omgeving onbruikbaar en is het erg moeilijk dit weer te herstellen. Om aan de Microsoft-behoefte toe te komen moet met regelmaat, bijvoorbeeld binnen iedere twee maanden, de omgeving worden opgebouwd zodat de synchronisatie kan plaatsvinden. Dit kan door deze harde schijf en de harde schijven van de andere servers in het domein, weer terug te plaatsen in een voertuig. Een andere mogelijkheid is het inrichten van een zogenaamd statisch synchronisatiedomein (server-rack) waarin met regelmaat deze synchronisatie plaatsvindt. Voor het ICMS-domein is zoiets dergelijks al ingericht bij het JCG.

Voordelen van deze *Starting Point*:

- het P&S-proces kan enorm bekort worden. Dit proces kunnen we dan het *Configuring and Provisioning* (C&P) proces noemen. Mijn inschatting is dat de benodigde tijd dan terugloopt tot 1 week C&P en 2 dagen systeemtest;
- nationale operaties kunnen direct ondersteund worden. De *Starting Point* schijf wordt meegenomen en *provisioning* vindt plaats op locatie;
- op de *Starting Point* omgeving staat geen missie of oefening gerelateerde data. Op deze wijze wordt dan voldaan aan de eis van de beveiligingsautoriteit;
- het maken van deze *Starting Point* kan worden teruggebracht tot het moment van uitbrengen van een nieuwe TITAAN *servicerelease*. Wanneer dit één keer per jaar is, kan ook de nodige *effort* worden gestoken in dit P&S-proces. Denkbaar is dat in dit geval de hulp van C2SC wordt ingeroepen om te komen tot een foutloos ingerichte omgeving. De *human-factor* wordt hiermee ook veel beter gecontroleerd en
- een *Starting Point* biedt ook de mogelijkheid om met veel minder voorbereiding op niveau 1 t/m 5 te trainen.

Een nadeel is de noodzakelijke synchronisatie. Het zou mooi zijn daar niet afhankelijk van te zijn en gewoon een *Starting Point* op een DVD gebrand te hebben. Wellicht toekomst?

Defecte hardware?
Met deze oplossing is nog geen oplossing gevonden voor het probleem dat veel hardware defect raakt bij het P&S-proces. Hiertoe is toch vrij eenvoudig een oplossing te bieden. De civiele apparatuur is ontworpen om 24/7 te draaien. Waarom dit ook niet toepassen in onze omgeving?
Dit betekent:
- servers niet op opslagverwarming maar op de volledige server-stack laten draaien en
- overige apparatuur, boxen, ook onder spanning in een kantoorachtige omgeving (luchtvochtigheid, temperatuur) opslaan.

Naast deze oplossing heeft C2SC op voordracht van 1GNC, contact gezocht met Hewlett Packard (HP). Na een bezoek aan het CISBn heeft HP toegezegd een onderzoek te starten om te komen tot een advies.

## WELKE INNOVATIE KUNNEN WE ZELF TOEPASSEN?

**Hosted unit**
Het instellen van de *First unit* naar de RACE is al een beoefend concept binnen het CISBn. Door schade en schande hebben we hierin geleerd dat het bijvoorbeeld erg belangrijk is om ook alle CIS-middelen toe te wijzen aan deze *First unit*. In de oefening COLD CHALLENGE gaf het ons vroegtijdig de mogelijkheid om de planning in CYRUS te starten. Maar goed ook, want deze oefening kenmerkte zich door grote onzekerheid over de deelnemende eenheden, waardoor het vaststellen van de ORBAT niet kon plaatsvinden.
Gewenst optreden onderkennen is hierin erg belangrijk. In de oefening COLD CHALLENGE is bijvoorbeeld het RACE van 1GNC, dat normaal gesproken de hooglaag-verbinding uitbrengt voor 43 MECHBDE, ondergebracht bij 1GNC-FWD. Dit bespaart ons een complete RACE wat mogelijk is vanwege de collocatie.

***Saven* van de situatie**
Het *saven* van de situatie is toch wat moeilijker. Voor het inrichten van een statisch synchronisatie domein is een investering benodigd. In deze tijd van bezuinigingen wat lastiger te realiseren.
Voor een statische situatie zijn servers benodigd als synchronisatie domein. Een alternatief is het gebruik van enkele servers als synchronisatie domein. Dit heeft als nadeel dat er altijd een server-paar beschikbaar moet zijn. Beide oplossingen vergen in ieder geval een strikte coördinatie, maar ook de beschikbaarheid van een grote set aan harde schijven. De oplossing is voorgesteld bij de G6 van 1GNC.

**Defecte hardware?**
Onze civiele hardware, ingebouwd in militaire voertuigen, is gebouwd om 24/7 te opereren. Om een vergelijking te maken; in mijn civiele tijd als projectmanager hield ik standaard al rekening met uitval van apparatuur op het moment dat het uitgezet werd voor een verhuizing. Het is hier dus gevoelig voor en wij doen niet anders! Aan de andere kant geven fabrikanten van apparatuur een *operating-environment* aan. Het bestaat uit de minimale en maximale temperatuur en de gewenste luchtvochtigheid. Om ook hier een vergelijking te maken; de server van het MCCC staat in een verwarmde loods opgesteld en draait 24/7. De MCCC-server vertoont sporadisch mankementen. Trek zelf uw conclusie.
Als nadeel moet worden opgemerkt dat deze procedure wel randvoorwaarden stelt aan de aanwezige infrastructuur en bij afwezigheid, de benodigde financiële ruimte om daarin te voorzien.

## VERANDERENDE KLANTBEHOEFTE

**Situatie**
De behoefte van de klant aan communicatie- en informatiesystemen die de processen ondersteunen, is de laatste jaren sterk gestegen. Dit is natuurlijk sterk ingegeven door de ontwikkelingen die de ICT zowel op de vredeslocatie als in de privéomgeving doormaakt.

**Operationeel internet**
Voorheen werd het NATO UNCLAS (NU) netwerk gebruikt om te communiceren met *Non-governemental Organizations* (NGO's) en *International Organizations* (IO's). Dit netwerk was niets anders dan een internettoegang met beveiliging en e-mailaccounts. NU wordt geleverd door bijvoorbeeld een *Deployabel CIS Module* (DCM) van NATO of door een eigen aansluiting. In geval van 1GNC worden de NATO-netwerken vanuit het HQ getunneld tot in de CP'n. De exacte bandbreedte was minder dan 256 Kbps. Niet echt van deze tijd dus.
De behoefte aan internet is enorm: als open source bron voor intel, nieuwsvergaring, fabrikantenondersteuning van civiele apparatuur maar ook ten behoeve van *Moral&Welfare*. De smalbandige toegang op internet via NU werd al snel vervangen door een eigen directe aansluiting op het internet, het netwerk 'operationeel internet'.
Alle apparatuur, kabels en overige middelen worden civiel aangekocht. Naast stand-alone aansluitingen worden ook al kleine netwerken ingericht met firewall, print- en opslagfaciliteiten.
Wanneer (breedbandig) internet niet direct op de locatie beschikbaar is, moet het worden verlengd vanuit een andere locatie. Op deze wijze hebben we in de oefening NEMESIS SWORD in 2009, op kamp Hörsten (Bergen, Duitsland) een 12Mbps internetaansluiting gerealiseerd. Voor de beheerder van het kamp was het de eerste keer dat hij het bordje 'internet café' zag staan op zijn kamp. Om gebruik te kunnen maken van e-mail, is er onder een centrale domeinnaam een webbased e-mailfaciliteit ingericht. Dit domein bevat ook de website van het 1GNC waarop een speciale pagina gewijd is aan de oefening en/of missie. Ook dit is in de laatste oefening als uitdrukkelijke wens geuit, om op die manier de internationale pers te informeren.

**Informatie delen**
Informatie delen door het naar elkaar te e-mailen, is al lang niet meer toereikend. De webserver WISE wordt gebruikt om informatie aan alle eenheden bekend te stellen. Ook krijgen eenheden de mogelijkheid om informatie te publiceren op deze WISE-server. De informatie die gedeeld wordt varieert van documenten van enkele KB tot presentaties en video's van tientallen MB.
Een toepassing die een grote vlucht heeft genomen is JChat. Dit chat-programma, *instant-messaging*, wordt vooral ingezet voor de snelle communicatie tussen operationele cellen van bijvoorbeeld 1GNC met divisies. JChat is ontwikkeld door NC3A van NATO.

**Welke innovatie is gewenst?**
Operationeel internet is een netwerk dat niet meer weg te denken is. Daarnaast groeit het in omvang tot een volwaardig netwerk. Het zou goed zijn om hier beleid in te formuleren dat aankoop, inrichting en beheer stroomlijnt. Er is behoefte aan apparatuur die de verschillende internetconnecties kan bundelen en beveiliging uitvoert.
Er is behoefte aan informatiedeling tussen verschillende TITAAN-eilanden. Deze informatie moet wel gereguleerd kunnen worden. Een bestand van 60MB downloaden van een centrale webserver zal onze smalbandige verbindingen snel verstoppen. Wanneer informatie gedeeld wordt met andere eenheden, is er behoefte aan integraal informatiemanagement. Wie is de eigenaar van de informatie, is het accuraat, etc. Dit is een zaak van informatiemanagement, maar niet onbelangrijk om te vermelden.
JChat wordt domeinoverschrijdend ingezet. Er is behoefte aan software die dit ondersteunt.

**Wat is er mogelijk?**
De keuze in civiele middelen die het operationeel internet ondersteunen is enorm. Er is behoefte aan apparatuur die eenvoudig te bedienen is. Stil in gebruik is ook een belangrijke voorwaarde, zo zijn er zogenaamde *low noise* bureauswitches verkrijgbaar. Ook in TITAAN zijn er al alternatieven ontwikkeld als stille variant op de LAB (LAN

Access Box). Deze behoefte groeit steeds meer omdat de apparatuur opgesteld staat in of nabij de werkruimte van de gebruiker. Gebruik van TITAAN-middelen zou de gewenste robuustheid kunnen verzorgen. Ik denk hierbij aan de fiberoptickabels met TITAAN LAB of LBB die gebruikt worden in de buitenbekabeling van het operationele internet. Internet kan verlengd worden door gebruik te maken van sterke civiele modems of *military of the shelve* (MOTS) modems, zoals de MRRS-straalzender.
Om te voorkomen dat gebruikers over WAN-middelen een centrale webserver benaderen, kan gedacht worden aan webservers per LAN die onderling gesynchroniseerd worden. Wanneer deze verkeersstroom dan ook gereguleerd kan worden, is synchronisatie ook mogelijk over smalbandige WAN-verbindingen.
JChat heeft niet stilgestaan in de ontwikkeling. De serversoftware kan nu meerdere domeinen ondersteunen.

**Welke innovatie kunnen we zelf toepassen?**
Het 'operationele internet' staat nog in de kinderschoenen. Beleid kan in eerste instantie ook eenvoudig op bataljonsniveau geformuleerd worden en pas later doctrinair worden verankerd. Inzet van TITAAN-middelen ter ondersteuning van dit netwerk vermindert de capaciteit die benodigd is voor het netwerk dat TITAAN ondersteunt. Hierin moet dus nog een besluit worden genomen of er behoefte is aan additioneel materiaal.
De inzet van de MRRS om internet te transporteren is erg succesvol gebleken in oefening NEMESIS SWORD, dit kunnen we dus zelf eenvoudig toepassen, mits beschikt kan worden over voldoende straalzender capaciteit.
De vraag om tot een werkbare oplossing te komen in het delen van informatie tussen domeinen, moet aan de ontwikkelaar, het C2SC, worden voorgelegd. De mogelijkheid van synchroniserende webservers is slechts een idee, wellicht zijn er veel betere oplossingen.
De nieuwe versie van JChat wordt op dit moment getest bij het CISBn. Omdat deze software ook als module is ingebouwd in de interface gateway box (IGB), zal er teruggekoppeld worden met C2SC.

## AFSLUITING

Per deelgebied heb ik getracht de centrale vraag 'welke innovatie kunnen wel zelf toepassen aan TITAAN' te beantwoorden. Een aantal innovaties moet door andere niveaus worden uitgewerkt.
De innovaties die wel zelf toegepast kunnen worden heb ik hieronder samengevat:
- het opzetten van een trust tussen domeinen;
- het gebruik van een niet gemodificeerde tunnelbox om TITAAN via internet te transporteren;
- instellen van de RACE als *first unit* zodat eenheden flexibel *hosted* kunnen zijn;
- TITAAN-servers 24/7 aanzetten en onderdak parkeren;
- initieel beleid formuleren op het netwerk operationeel internet;
- de MRRS inzetten om internet te transporteren.

Met dit artikel heb ik u geïnformeerd over de ontwikkelingen in TITAAN, die ervaren zijn na het een aantal jaren gebruikt te hebben. Een aantal gebieden kent innovaties die door ons als gebruiker, eenvoudig toepasbaar zijn. Voor de andere beschreven gebieden zijn er ideeën die voorgelegd zijn op andere niveaus. Mocht hiermee een discussie gestart zijn waar we heen moeten met de ontwikkeling van TITAAN, dan is ook dat doel bereikt!

# NAWOORD C2SC

**In het artikel '1GNC; een veranderende omgeving, innovatiekansen' heeft de auteur, kap Van de Braak, een aantal directe en indirecte verwijzingen naar het C2SC, de bouwer van TITAAN, opgenomen. De redactie heeft de Commandant van het C2SC, kol J.P.L. Duckers, gevraagd om een reactie en hij was daartoe graag bereid.**

Allereerst wil ik de kap Van de Braak complimenteren met zijn artikel. Behalve het signaleren van problemen doet hij suggesties voor mogelijke oplossingen die wij zeker zullen meenemen. Vanuit het C2SC-perspectief enkele kanttekeningen.

## PRIMING &STAGING

Allereerst het onderkende Priming &Staging probleem. Dit is voor mij ook een doorn in het oog. Het vergt te veel capaciteit om het systeem voor te bereiden op inzet. De hardware situatie ("oud", kwetsbaar zonder juiste opslag etc.) en alles wat daarbij komt kijken is de reden dat we in de volgende versie van TITAAN proberen los te komen van de hardware. Dit zal nooit volledig kunnen, maar de afhankelijkheid van het systeem met de actieve hardware componenten moet drastisch worden verminderd.

## OPERATIONELE EISEN

Wat we echter niet moeten vergeten is dat het ontwerp van TITAAN is gebaseerd op operationele eisen voor het voeren van de meest veeleisende inzetvorm. Deze inzetvorm gaat uit van een mobiel grootschalig expeditionair gemechaniseerd optreden in het hogere deel van het geweldspectrum. De gestelde eisen en de gekozen oplossing maken TITAAN 4 zeer complex. Deze complexiteit kent zijn weerslag in de benodigde management en de beheerscapaciteit. In deze problematiek is het zaak een balans te vinden tussen generieke functionaliteit en flexibiliteit. De richtlijn voor het ontwerp van TITAAN 5 is meer uitgaan van generieke functionaliteit: Goed is goed genoeg. Daarnaast moeten we als Krijgsmacht de functionele behoeftes herijken en valideren aan toekomstig optreden.

## BANDBREEDTE

Een ander belangrijk punt dat de kap Van de Braak aanhaalt is de benodigde bandbreedte. De behoefte aan bandbreedte vertoont overeenkomsten met het fileprobleem. Meer asfalt gaat alleen fileoplossingen bieden als de hoeveelheid auto's niet toeneemt en de tijdstippen waarop de auto's gebruikt worden niet meer pieken vertonen. De beschikbare bandbreedte zal in de toekomst wel toenemen, maar de behoefte hieraan door nieuwe gebruikers zullen net zo snel of nog sneller groeien. Voorbeelden hiervan zijn al geschetst door de kap Van de Braak, maar ook kostenbesparende maatregelen zoals SAP en Tele Maintenance vragen om bandbreedte.

## ILIAS EN ENII

Voor de toekomst is het dus zaak om effectiever om te gaan met de beschikbare bandbreedte. Voor expeditionair optreden zal veelal gebruik gemaakt worden van satellietcommunicatie. In het nieuwe ontwerp van TITAAN 5, de nieuwe applicaties binnen ILIAS (de in 2013 uit te brengen applicatiesuite) en de nog uit te werken Expeditionaire Netwerk Informatie Infrastructuur (ENII) moeten we simpelweg minder bandbreedte consumeren om zo extra ruimte te creëren voor additionele behoeftes voor toekomstig militair optreden binnen een geïntegreerde aanpak (Comprehensive Approach). Ondanks dat zullen er altijd afwegingen gemaakt moeten worden.

Tot slot wil ik de kap Van de Braak vragen om regelmatig zijn ervaringen en ideeën met het C2SC te blijven delen. Dergelijke input is zeer welkom en draagt substantieel bij in het bewandelen van de nieuwe weg van het C2SC richting een ENII.