COLD CHALLENGE 2011 OVER INTERNET

Luitenant-kolonel Kees Verdonk en majoor Dennis van de Braak, HRFHQ/CISBn

Van 17 tot 31 maart 2011 heeft 1 (GE/NL) Corps deelgenomen aan de oefening COLD CHALLENGE 11 (CC11) als staf van een *Land Component Command* (HQ LCC). Het doel van de oefening was 43 Mechbrig en een Noorse brigade te trainen in het noorden van Noorwegen. Vanuit Nederland nam staf 11 AMB deel aan de oefening. In dit artikel informeren de auteurs u over de CIS-ondersteuning van de oefening in het algemeen en over het gebruik van internet als verbindingsmiddel in het bijzonder. Het artikel is dan ook opgebouwd uit twee delen. Ik het eerste deel beschrijft lkol Verdonk de algemene opzet van de oefening, de benodigde CIS-ondersteuning, de resultaten en ervaringen van de oefening. In het tweede deel gaat maj Van de Braak (CISBn/S3/C-MCCC) nader in op het gebruik van internet als WAN-middel. Wordt met internet het Paard van Troje binnengehaald en juichen we dus te vroeg? De toekomst zal moeten uitwijzen in hoeverre onze TITAAN-servers en TITAAN-clients bestand zijn tegen de cyberdreigingen van onze tijd.

DE CIS-ONDERSTEUNING VAN DE OEFENING COLD CHALLENGE 11

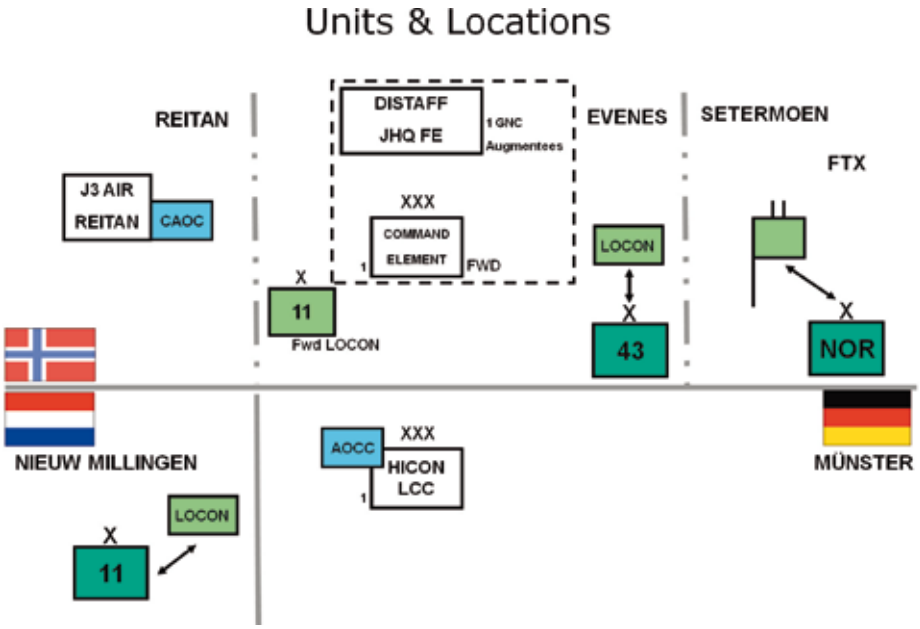
De opzet van de oefening

Tijdens de oefening testte de staf 1 (GE/NL) Corps onder meer het zogenaamde Reach Forward-concept, waarin het merendeel van de LCC-staf (Main/HICON LCC) de oefening ondersteunde vanuit de vredeslocatie in Münster (Duitsland) en de commandant, lgen Van Loon, met een klein stafelement (*Command Element/Fwd*) optrad in het oefengebied van Noord-Noorwegen. Op deze wijze werd de fysieke aanwezigheid (*footprint*) van het HQ LCC zoveel mogelijk verkleind zonder dat de aansturing van operaties (C2-structuur) door HQ LCC in het oefengebied werd beperkt. Dit betekende wel dat *LCC Main* en het *Command Element* altijd over exact dezelfde informatie moesten beschikken. Kijkende naar deze opzet van de oefening had de commandant 1 (GE/NL) Corps al in de voorbereiding aangegeven dat de CIS-ondersteuning essentieel zou zijn voor de uitvoering van de oefening.

De CIS-ondersteuning

Het CIS Battalion 1 (GE/NL) Corps had de opdracht om de oefenende eenheden in Nederland, Duitsland en Noorwegen van een groot aantal CIS-diensten (*services*) te voorzien zoals telefonie (VOIP), e-mail (Outlook), het informatiesysteem HEROS (het Duitse ISIS), internet en verder een groot

Figuur 2: Aoo Vrijenhoeff tijdens de wintertraining bij de NORBDE



Figuur 1: Eenheden en locaties in oefening COLD CHALLENGE 11

Figuur 3: TITAAN voertuigen in de sneeuw bij 20 graden onder nul

Figuur 4: De tactische trailer wordt op de zeecontainers geplaatst

aantal specifieke Corps- en NATO-toepassingen (MILGEO, ICC Light (luchtplaatje), JOCWatch, JChat (chatprogramma), etc.). Vanwege de lange afstanden tussen de staven bestond er bij commandanten en stafpersoneel een grote behoefte om elkaar te kunnen spreken èn te kunnen zien. Dit betekende dat er een groot aantal *Video-Tele-Conference* (VTC)-sessies zouden worden gehouden waarin de deelnemers elkaar op vijf locaties gelijktijdig moesten kunnen zien en spreken (multi-point VTC). Daarnaast werd tijdens de oefening duidelijk dat er op de laatste oefendag een extra VTC-verbinding met Staf CLAS in Utrecht moest worden gerealiseerd.

De installatie en het beheer van de lokale netwerken (LAN, *Local Area Network*) bij de deelnemende staven werd door de RACEs (*Rapid CIS-Elements*) uitgevoerd. Daarbij moesten verschillende RACEs met hun TITAAN-materieel worden ingezet onder arctische omstandigheden bij temperaturen lager dan -20 gr Celsius. Ook het personeel moest worden getraind in het overleven in ijzige omstandigheden met daarbij extra aandacht voor de chauffeurs die over de veelal besneeuwde en bevroren wegen moesten rijden.

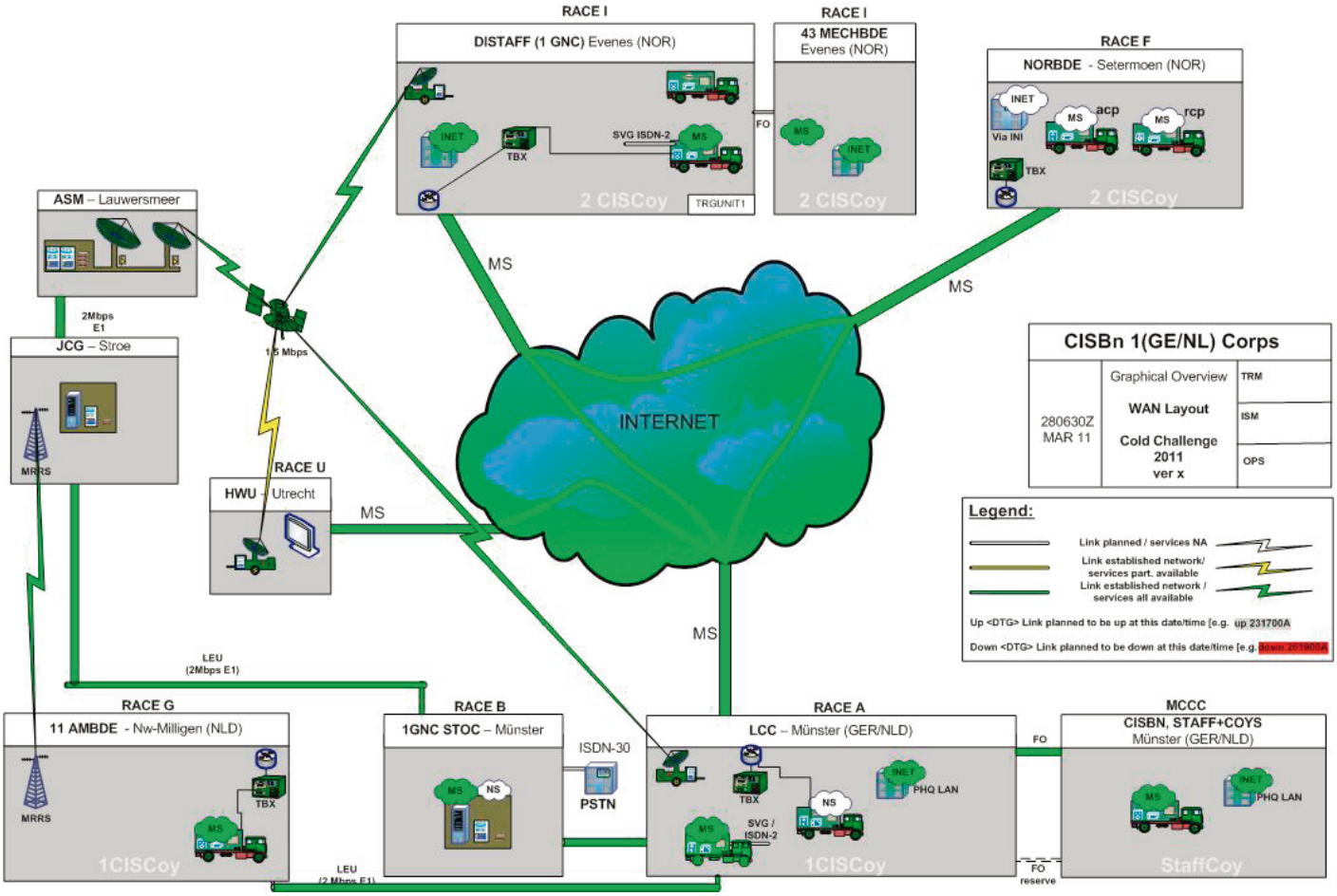
Figuur 5: De tactische trailer stevig vastgezet op de zeecontainers waardoor satcomverbinding met Noord-Noorwegen mogelijk werd. (Zie de lage opstraalhoek van de schotel)

Bij de koppeling van de LANs in verschillende landen in één *Wide Area Network* (WAN) waren er verschillende uitdagingen. Mede door de opsplitsing van staf LCC in twee delen en de behoefte aan *multipoint* VTC zou er veel dataverkeer gaan ontstaan tussen de LANs. De transmissiemiddelen moesten dus in staat zijn grote hoeveelheden data te verzenden (breedbandig). Door de grote afstanden tussen de LANs was het gebruik van de nieuwe straalzender *Mobile Radio Relay System* (met een bereik van 30-40 km) nauwelijks mogelijk. Ook het gebruik van het satellietcommunicatiesysteem (tactical trailer-TT) in Noord-Noorwegen was zeer onzeker omdat de opstraalhoek van de satellietschotel naar de satelliet boven de evenaar slechts 7 graden bedroeg, waardoor de bergen een 'vrij zicht' tussen de schotel en de satelliet zouden belemmeren. Uiteindelijk lukte het op één locatie (Evenes) in Noorwegen de satellietverbinding tot stand te brengen door de satellietrailer op twee zeecontainers te plaatsen. Dit leverde echter een beperkte bandbreedte op (1,5 Mbps) om de oefening te kunnen ondersteunen.

Ten slotte bleken de geplande vaste lijnen tussen Noord-Noorwegen en Nederland en Duitsland niet tijdig beschikbaar. Wel was er in het oefengebied voldoende breedbandinternet beschikbaar. Daarom is tijdens de oefening voor het eerst op grote schaal gebruik gemaakt van het internet als beveiligd transmissiemiddel om de LANs met elkaar te verbinden. In het tweede deel van het artikel licht majoor Van de Braak deze optie nader toe. Als tweede back-up verbinding werden de middelen uit de RECCE (*reconnaissance* ofwel verkenning)-packs beschikbaar gehouden. Het gaat hierom de R-BGAN (kleinschalige satelliet internettoegang) en Iridium-satcom (satellietelefonie).

De resultaten en ervaringen

De CIS-ondersteuning met het TITAAN-systeem is op uitstekende wijze verlopen. Zo had het systeem nauwelijks last van de strenge vorst en de vele sneeuw in Noorwegen. Ook de satcominstallatie op de zeecontainers was bestand tegen de sneeuwstormen. Na enkele opstartproblemen heeft het internet als belangrijkste verbindingsmiddel uitstekend gefunctioneerd. De verbinding was stabiel en leverde de benodigde bandbreedte. Ook de VTC-verbinding naar Staf CLAS is via het internet gerealiseerd (met dank aan het C2CoE). Daarnaast is er veel gebruik gemaakt van de VTC. Van de 13 oefenuren per dag werd gemiddeld zes uur gebruik gemaakt van *multi point* VTC. In tegenstelling tot eerdere oefeningen functioneerde de nieuwe VTC-apparatuur naar volle tevredenheid en vrijwel zonder haperingen.



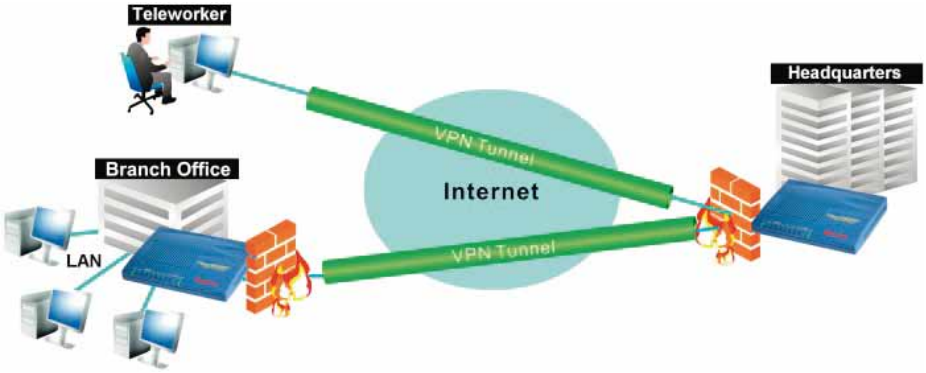
Figuur 6: WAN overzicht COLD CHALLENGE 11

Verder werd tijdens de oefening duidelijk dat de hoeveelheid dataverkeer enorm toeneemt door onder meer het gebruik van de VTC, de splitsing van hoofdkwartieren en het grote aantal (grafische) applicaties. Hoewel de nieuwe MRRS de mogelijkheid heeft om grote hoeveelheden data in korte tijd te verzenden, is de relatief korte afstand een beperking. Ook blijkt uit de oefening dat de TT niet overal ingezet kan worden en dat de bandbreedte van dit verbindingsmiddel een beperkende factor gaat worden. Dit onderwerp zal in de (nabije) toekomst steeds nadrukkelijker naar voren komen. Daarom bekijkt G-6 1 (GE/NL) Corps inmiddels op welke wijze het dataverkeer tussen de staven kan worden teruggebracht. Op dit moment wordt ook onderzocht hoe er zoveel mogelijk bandbreedte kan worden vrijgemaakt door creatief gebruik van de (lokaal) beschikbare verbindingsmiddelen (TT, lijn, internet, MRRS, etc.).

Daarnaast werd het tijdens de oefening duidelijk dat veel kennis over TITAAN en de Corps/NAVO-softwareprogramma's op het laagste zelfstandige niveau (de RACE's) aanwezig moet zijn. RACE's worden met staven meegezonden en staan op duizenden kilometers van elkaar. Problemen met het LAN, een applicatie of een transmissiemiddel (zoals de koppeling via internet) kunnen lang niet altijd *remote* worden opgelost. RACE's moeten in staat zijn problemen zelfstandig op locatie te kunnen oplossen. Vaak heeft het RACE-personeel daarom meer kennis nodig dan in hun functiebeschrijving staat. De continue opleiding en training van personeel is essentieel, bijvoorbeeld door het experimenteren met de mogelijkheden (en beperkingen) van TITAAN en internet op de dagelijkse werkplek.

Ten slotte is de CIS-ondersteuning pas echt succesvol als ook de TITAAN-gebruikers tevreden zijn. De reacties van de veelal internationale deelnemers over de CIS-ondersteuning waren bijzonder positief. Zij waren zeer te spreken over het TITAAN-systeem vanwege de eenvoud in gebruik, de vele mogelijkheden en de snelheid van het systeem. Zonder enige TITAAN-kennis waren buitenlandse deelnemers in staat de eindapparatuur te gebruiken. Ondanks enige kleine

Figuur 7: De TCE-C van de firma Thales



Figuur 8: Remote access VPN en site-to-site VPN

problemen voorzag Outlook (in plaats van Themis) in een belangrijke behoefte van de TITAAN-gebruikers om eenvoudig informatie met elkaar uit te wisselen. In zijn afsluitende briefing benadrukte de commandant 1 (GE/NL) Corps nogmaals het belang van een goede CIS-ondersteuning voor een goed functionerende *Command & Control*-structuur zodat belangrijke informatie tijdig kan worden verspreid. Lgen Van Loon ziet de CIS-ondersteuning daarom als een kerntaak van 1 (GE/NL) Corps.

Terugkijkende op het verloop van de oefening en de reactie van deelnemers kan men concluderen dat de Verbindingsdienst met het TITAAN-systeem haar meerwaarde in een multinationale omgeving wederom heeft bewezen.

INTERNET ALS DRAGER

Inleiding
Zoals in het vorige deel is vermeld, is tijdens de oefening CC11 voor het eerst bij 1 (GE/NL) Corps op grote schaal gebruik gemaakt van het internet. Het internet werd voornamelijk gebruikt om de commandoposten (CP'n) van de eenheden in Noorwegen te verbinden met de CP'n in Nederland en Duitsland.

In dit deel wil ik u informeren over het gebruik van internet als drager. Ik zal dat doen aan de hand van de centrale vraag; Is het internet een geschikte drager (transmissiemiddel) voor het operationele netwerk TITAAN? Om deze vraag te beantwoorden zal ik formuleren welke eisen we zouden willen stellen aan een drager. Verder zal ik beschrijven wat het internet kan bieden met een onderzoek tot bedrijven die hun dragend netwerk aan openbare netwerken hebben toevertrouwd. Dit alles resulteert in een conclusie en een afsluitend commentaar met als doel de opname van internet als drager, WAN-element van TITAAN.

Het gebruik van internet in de oefening COLD CHALLENGE van 1GNC
Voordat de oefening plaatsvond heb ik u hierover geïnformeerd in het artikel 'Een veranderende omgeving, innovatiekansen' (Intercom 2011-1, blz. 37 e.v., red). Een fantastisch resultaat is behaald in deze oefening! Er stonden stabiele WAN-verbindingen via het internet met CP'n in twee landen, de REACH-FWD CP 1GNC, CP 43 MECHBDE en CP NORBDE in Noorwegen en MAIN CP 1GNC in Duitsland. De CP 11 AMBDE in Nederland was via satellietcommunicatie, de nieuwe MRRS en een vaste lijn in het WAN opgenomen. TITAAN versie 4.1 servicerelease 4 werd gebruikt en er was sprake van veel data-uitwisseling van services, die een hoge kwaliteit en beschikbaarheid vereisen, zoals *Video-TeleConference* (VTC). Als klapstuk vond er een VTC plaats ter evaluatie van de oefening met de commandant, lgen Van Loon, in Noorwegen en de brigadecommandanten bij Staf CLAS. In totaal een 5-multipoint VTC d.w.z. vijf deelnemers in deze sessie met een gemiddeld bandbreedte gebruik van 1 Mbps, uitgebracht via internet.
De verbinding, bestaande uit een Cisco PIX-firewall en een TCE621 cryptoapparaat voor additionele beveiliging, is uiteindelijk redelijk eenvoudig opgezet. De TCE621-N zoals we die nu hebben in de tunnelboxen, voldeed niet in vercijfersnelheid voor de gewenste bandbreedte. Voor de verbinding van de FORWARD-CP 1GNC in Noorwegen met de MAIN-CP 1GNC in Duitsland, was een bandbreedte van minimaal 2 Mbps vereist. Dit vanwege de 'trust-relatie' tussen de CP'n die gerealiseerd werd. Met hulp van het C2SC is de TCE621-C ingezet, die een veel hogere vercijfercapaciteit kent. Deze C-versie is tevens geaccrediteerd voor gebruik van de gewenste beveiligingswaarde[1]. Dit net zoals de B-versie, die beschikbaar is in een pool van de DEFDA.

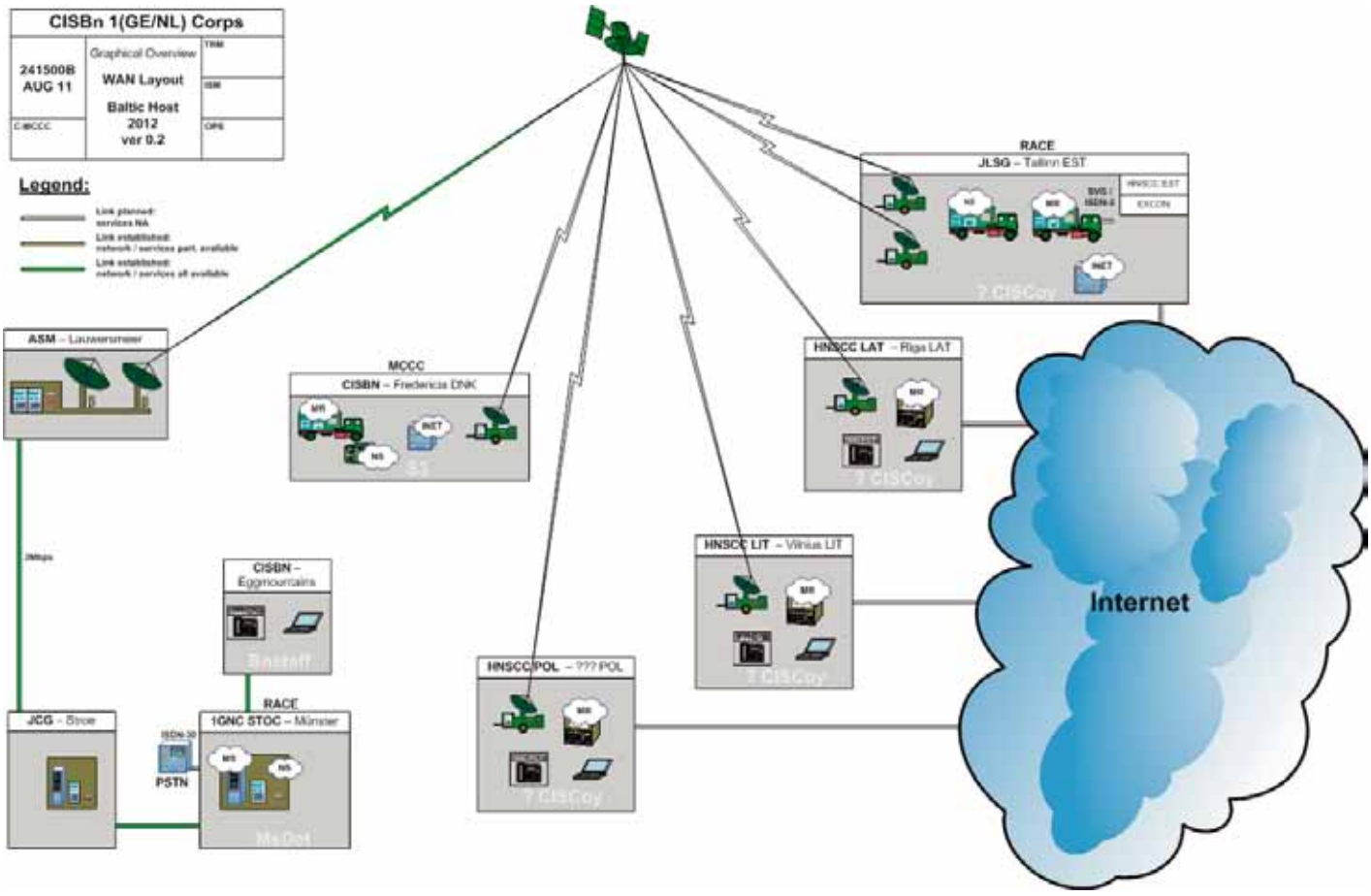
Welke eisen stellen we aan de drager functie?
Volgens de informatiebeveiligingsregels eisen we dat de drager betrouwbaar is. Dit is bijna traditioneel onder te verdelen in het volgende:
- Hoge beschikbaarheid, korte uitvaltijd en uitbreidbaar met meerdere routes (redundantie).
- Integer, dat wat ik zend moet onveranderd bij de ontvanger aankomen.
- Exclusief, niet toegankelijk voor onbevoegden, bijv. vercijfering.

Beschikbaarheid. In optimale netwerkontwerpen van TITAAN wordt altijd een back-up WAN-middel gepland. Middels kostberekening wordt door het TITAAN-systeem de meest efficiënte route berekend, maar zijn bij uitval van deze route de alternatieve routes bekend. Daarnaast kunnen straalzender-, satcom-, en lijnverbindingen stabiel ingeregeld worden. Deze MOTS[2] WAN-verbindingen binnen TITAAN hebben zich bewezen als stabiele verbindingen met een hoge beschikbaarheid.

Integriteit. TITAAN heeft in zijn buitenschil, de access, voorzieningen die ervoor zorgen dat het niet eenvoudig is om toegang te verkrijgen tot het netwerk. Integriteit wordt ook bereikt door routering aan te passen. Als we stellen dat we alleen van A met B willen praten dan is het uitgesloten dat C en volgend, een antwoord krijgt. Een en ander is in de netwerklagen in te regelen bijvoorbeeld met *ACL's*[3] *en null-routing*[4]. Ook moet er beveiliging bestaan tegen het fenomeen *man in the middle*, waar de data verandert zonder dat het opgemerkt wordt. Maatregelen kunnen zijn: controle-getallen, PKI-certificaten en vercijfering.

Exclusiviteit. Data die geclassificeerde informatie bevat mag niet in handen van onbevoegden komen. Hiertoe dient de data vercijferd te worden met apparatuur dat daartoe ook de accreditatie heeft. Wanneer data over openbare netwerken getransporteerd wordt, is dit een belangrijk punt.

WAT KAN HET INTERNET BIEDEN?
Het internet is een wereldwijd openbaar computernetwerk. Het is zeer toegankelijk via diverse aansluitmogelijkheden en zeer fijn vermaasd, zodat bij uitval van routes er bijna altijd een alternatieve route beschikbaar is. De beschikbare bandbreedte is enorm vergeleken met onze TITAAN WAN-middelen.
In de jaren 90 werden dure huurlijnen en/of ISDN gebruikt om de netwerken van bedrijven van verschillende vestigingen aan elkaar te verbinden. Met de komst van internet is het mogelijk een *Virtual Private Network* (VPN) te realiseren. Dit VPN is een beveiligde, privé (*dedicated*) verbinding over een openbare infrastructuur.
Een VPN kan met verschillende protocollen worden opgezet over bijna iedere gangbare TCP/IP-infrastructuur. Grote telecomproviders bieden hun private infrastructuur hiervoor aan waarop dan ook nog de ge-



Figuur 9: Oefening Baltic Host 2012

wenste *quality of service* (QoS)[5] geleverd kan worden. Als voorbeeld de RABO-bank die middels VPN gebruik maakt van KPN's Epacity-netwerk. Een van de grootste implementaties van VPN met ongeveer 1600 vestigingen en bijna 3000 geldautomaten. Op het openbare internet kan deze QoS niet geleverd worden. Hier wordt het voornamelijk gebruikt om thuiswerkers te faciliteren en met *business partners* informatie uit te wisselen. Afhankelijk van de te transporteren services is een VPN zonder QoS, dus over internet, zeker een optie. We kunnen dus twee soorten VPN's onderkennen, de *remote-access VPN's* en *site-to-site VPN's* die gehost kunnen worden op een netwerkinfrastructuur van een provider of het internet. Een voorbeeld waar ik intensief bij betrokken ben geweest is het JustitieNet2-netwerk. Dit netwerk is gehost op de infrastructuur van Versatel (nu Tele-2) en heeft additionele vercijferapparatuur direct achter de WAN-netwerkcomponenten. Juist dit ministerie stelt hoge eisen aan de exclusiviteit en heeft deze implementatie geaccrediteerd. Andere bedrijven maken gebruik van het openbare internet. Relatief goedkoop kunnen hier wereldwijde netwerken gebouwd worden. Zeker bij gebruik van grote bandbreedtes wordt een fluctuatie in het netwerk (internet) eenvoudig opgevangen.

VPN wordt ook wel *tunneling* genoemd, net zoals bij het 1GNC waar het *Nato Secret* netwerk over het *Mission Secret* netwerk getransporteerd wordt. Weliswaar zijn er verschillende *tunneling* technieken, maar binnen VPN over het internet wordt veelal het IPsec protocol gebruikt. De *tunneling* techniek waar binnen TITAAN van gebruik wordt gemaakt is gebaseerd op het *multi cast*-principe. Een zeer innovatieve oplossing, die goed werkt binnen TITAAN. Daar *multicasting* niet wordt toegepast op het internet is dit principe daar niet toepasbaar. Het internet biedt dus voldoende mogelijkheden en is ook zeer wijd toegankelijk. Dit brengt automatisch met zich mee dat het ook toegankelijk is voor personen die kwaad in zin hebben. Hier moeten we ons beschermen door de informatie exclusief te houden. De eerdere gestelde ACL en *null-routing* bieden een oplossing. Op deze manier stellen we vrij zeker dat we communiceren met de gewenste tegenpost, alle niet gedefinieerde tegenposten worden genegeerd. En hoe dan te wapenen tegen de hedendaagse moderne aanvalstechniek, de (D)DOS[6]? Deze techniek kan alleen worden toegepast op een internetomgeving die voor iedereen bereikbaar moet zijn (bijv. een website). Een website van een overheid bijvoorbeeld moet wel voor iedereen bereikbaar zijn en dus ook diegenen die kwaad in zin hebben. Onze situatie is niet vergelijkbaar met een omgeving die vanuit elke computer bereikbaar moet zijn. Daarom kunnen 'wij' ons tegen een (D)DOS dus redelijk eenvoudig beschermen.

Het is de vraag of de toegankelijkheid tot het internet ook bestaat in de gebieden waar een mogelijke missie kan plaatsvinden. Een eenvoudige *web search* op het internet leert dat iedere grotere stad, ook in de derde wereldlanden, wel over internet beschikt. Al zouden we voor een missie alleen maar de *Home Base Link* (HBL) via het internet realiseren, dan hebben we hier al winst geboekt. Natuurlijk realiseer ik me dat deze beschikbaarheid erg onzeker is in tijden van onrust. Dit zien we op dit moment ook terug bij de onrust in Libië. In de hoofdstad Tripoli valt het internet regelmatig uit. Lokaal internet is dan ook meer een optie in een stabiliserende fase.

Financieel gezien is een toegang tot internet in vergelijk met huurlijnen een fractie van de kosten. Huurlijnen kosten al gauw enkele duizenden euro's per maand. Een businessaansluiting[7] komt op een paar honderd euro per maand.

CONCLUSIE

Is het internet een geschikte drager voor het operationele TITAAN-netwerk? Ja, mits een stabiel internet beschikbaar is en gebruik gemaakt wordt van grote bandbreedtes.

Daarnaast is het ook budgettair interessant. Niet alleen TITAAN kan hiervan profiteren maar ook het in de toekomst te realiseren ENII-netwerk[8]. De beschikbaarheid is tegenwoordig hoog te noemen en de exclusiviteit met additionele vercijferapparatuur op het gewenste niveau.
Om eenvoudig te beschikken over middelen om dit te faciliteren zouden bijvoorbeeld enkele tunnelboxen geüpdatet kunnen worden met een moderne TCE621, versie B of C. Met additionele documentatie voor de configuratie is het compleet.
'Eén verbinding is geen verbinding', blijft van kracht. Traditionele WAN-middelen, zoals Satcom en vercijferde geschakelde verbindingen, moeten blijven bestaan naast een internet WAN-middel. Internet is dus geen vervanging maar een waardevolle aanvulling op de bestaande WAN-middelen.
In de planning van het netwerk is het belangrijk om te realiseren dat de beschikbaarheid van internet afhankelijk is van derden. Dit geldt overigens ook voor huurlijnen (de zogenaamde LEU[9]-verbinding). Satellietcommunicatie is in vergelijk minder afhankelijk en zal daarom een hoofdverbindingsmiddel blijven.

AFSLUITING

Met dit artikel heb ik met u mijn gedachten en ervaringen over het gebruik van internet als drager willen delen. Ik wil hiermee bijdragen aan een formalisatie van het gebruik van internet. Een reactie is altijd bijzonder welkom, positief of negatief. Daartoe kunt u contact met mij opnemen via de bij defensie bekende weg.

In juni 2012 zal het CISBn de oefening BALTIC HOST 12 van het RSC[10] ondersteunen in de Baltische staten in het kader van *host nation support*. In Estland, Letland, Litouwen en Polen zullen TITAAN-LAN's met elkaar verbonden worden via VPN over internet. Satcom is hier niet het hoofd-verbindingsmiddel maar een back-up. Ter illustratie figuur 9.

VOETNOTEN EN BRONNEN

1. Voor meer informatie zie https://www.aivd.nl/organisatie/eenheden/nationaal-bureau/artikel/goedgekeurde/
2. *Military Of The Shelf* d.w.z. defensieontwikkeling
3. Access Control List
4. Al het onbekende verkeerde gaat naar een *null*-route, 'vloeit' weg, wordt niet op gereageerd.
5. QoS, bijvoorbeeld door het gebruik van MPLS (*Multi Protocol Label Switching*)
6. (Distributed) Denial Of Service
7. 1 op 1 verbinding, niet gedeeld met anderen. Een eigen publiek IP-adres (*fixed IP*)
8. *Expeditionaire Netwerk Informatie Infrastructuur*
9. *Line Encryption Unit*
10. *Rear Support Command* van 1GNC

CARTOON

Onze hoofdredacteur in Jeruzalem