COMMON EFFORT

Kapitein Jeroen Lalleman,
Ops Officer binnen de Sectie 3 van het CISBn

Van 19 tot en met 23 september 2011 heeft de oefening Common Effort plaatsgevonden in Münster, Duitsland. Deze oefening sloot het project Common Effort af dat in september 2010 begon. Binnen dit project werkten de Ministeries van Buitenlandse Zaken van Duitsland en Nederland, 1(GE/NL) Corps (1GNC) en een groot aantal civiele (hulp-) organisaties samen aan het in de praktijk brengen van het concept van de Comprehensive Approach om daarmee gezamenlijk conflicten in de wereld effectief aan te pakken. Over zowel het project als de oefening heeft u in verschillende bladen al artikelen kunnen lezen. In dit artikel zal kap Lalleman u een beeld schetsen van de opzet van de oefening Common Effort 11 en van de CIS ondersteuning die voor de oefening is geleverd door het (NLD/DEU) CIS Battalion, dat deel uitmaakt van 1 GNC.

DE COMPREHENSIVE APPROACH

Hedendaagse conflicten, zoals in Afghanistan, zijn complex. Vaak is er gelijktijdig sprake van een gewapend conflict, een zwakke rechtsstaat en heerst er grote armoede. Dergelijke conflicten worden niet opgelost door militair ingrijpen alleen. De rol van civiele, (non-)gouvernementele organisaties (zoals de VN, het Rode Kruis, ministeries uit verschillende landen) en lokale autoriteiten in het vinden van een blijvende oplossing voor conflicten is zeer belangrijk. De ervaring leert dat het niet vanzelfsprekend is dat militairen, hulpverleners, diplomaten en lokale bestuurders dezelfde doelen nastreven of uitgaan van gelijke principes. Het effectief aanpakken van crises betekent echter wel dat alle spelers op de hoogte moeten zijn van elkaars werkwijzen en plannen. Om dit mogelijk te maken, is een geïntegreerde analyse van een crisis en (waar mogelijk) de gezamenlijke planning en uitvoering van activiteiten van groot belang. Tijdige afstemming van elkanders activiteiten leidt tot een effectievere aanpak van de crisis en voorkomt veel onbegrip en frustratie bij de spelers in het inzetgebied.

Mede om deze reden is de uitwisseling van informatie tussen de verschillende spelers zeer belangrijk. Als voorbeeld ontving de huidige commandant 1 (GE/NL) Corps, lgen van Loon, tijdens zijn ISAF-uitzending als Commandant RC-South (in 2006 – 2007), een melding dat eigen troepen in een hinderlaag van de Taliban waren gereden. Hij had verder informatie dat op deze weg ook een civiel hulpkonvooi in de richting van de hinderlaag reed. Echter, het militaire CIS-netwerk waarover C-RC South destijds beschikte, had onvoldoende mogelijkheden om de hulporganisatie tijdig voor de hinderlaag te waarschuwen met alle gevolgen van dien. Deze gebeurtenis toont opnieuw aan dat een goede uitwisseling van informatie tussen militaire eenheden, regerings- en civiele (hulp-)organisaties essentieel is.

Onder het motto *We believe cooperation should start before we meet abroad in a crisis* is in september 2010 het project Common Effort in het leven geroepen door 1GNC waarbij de ministeries van Buitenlandse Zaken van beide landen zich hebben aangesloten. Vervolgens is men gezamenlijk aan de slag gegaan om andere organisaties te benaderen om zich ook bij dit project aan te sluiten. En met succes, verschillende universiteiten (Regensburg, Münster, e.a.), hulporganisaties (UNHCR, CORDAID, Deutsches Rotes Kreuz, e.a.), diplomaten en politie hebben zich bij het project aangesloten. Een jaar later, in september 2011, werd het sluitstuk van het project bereikt met de oefening Common Effort.

Van 19 tot en met 23 september kwamen 146 civiele en 311 militaire deelnemers bijeen op de Manfred von Richthofen (MvR) kazerne in Münster. Tijdens de oefening werd een crisis in het fictieve land Tytan gebruikt als achtergrond voor de eerder genoemde geïntegreerde aanloop van de crisisaanpak; de Comprehensive Approach werd hier in de praktijk gebracht. 1 GNC trad daarbij op in de rol van HQ Land Component Command (LCC).

EEN NIEUW CP CONCEPT

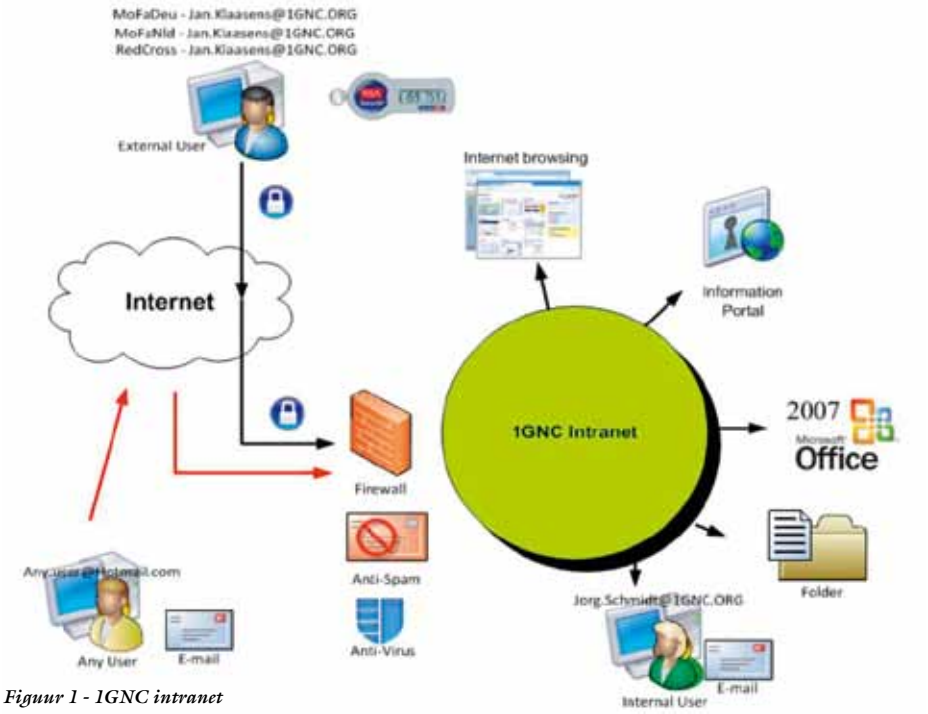
De invoering van het Comprehensive Approach-concept leidde ook tot een nieuw commandopost (CP)-concept, het zgn. 'open CP'-concept. De CP heeft een belangrijke taak: het delen van informatie. Vóór de oefening Common Effort was dit relatief eenvoudig. De staf ontwikkelde plannen en leidde de operatie vanuit de CP. Bovendien moest de staf in staat zijn zowel onderling als met het hogere en het lagere militaire niveau te communiceren. Dit alles vond plaats in een gesloten (TITAAN-)omgeving om toegang tot deze informatiestroom aan de vijand te ontzeggen.

Met de actieve samenwerking met niet-militaire organisaties is de behoefte ontstaan om informatie te delen met deze 'externen' met als credo *from need to know to duty to share*. Bij een daadwerkelijke inzet zal het overgrote deel van de civiele organisaties niet fysiek deel uit maken van de CP-bezetting, maar op afstand informatie delen. Om dit mogelijk te maken is een CIS-netwerk opgezet dat via het internet te benaderen is en waarop militairen, hulpverleners en diplomaten hun informatie kunnen delen. De naam voor dit nieuwe netwerk is 1GNC-intranet (zie figuur 1) en heeft de classificatie NATO UNCLASSIFIED.

Vanwege de experimentele aard van de oefening bevonden in dit geval wel alle civiele deelnemers zich in het zelfde gebouw als de CP van 1 GNC. Hiervoor was de CP opgedeeld in een afgeschermd deel, van waaruit de militaire operatie werd geleid, en een open deel waar de gezamenlijke analyse en planning plaatsvond met de civiele deelnemers. Op de MvR-kazerne is het gesloten TITAAN-netwerk MISSION SECRET uitgebracht voor de uitwisseling van geclassificeerde militaire informatie en het 1GNC-intranet voor de informatie-uitwisseling met civiele organisaties. Als test waren er op verschillende locaties buiten de CP ook civiele gebruikers van het 1GNC-intranet die via het internet, op het 1GNC-intranet in konden loggen. Dat betekende onder meer dat personeel van het Ministerie van Buitenlandse Zaken in Den Haag via het internet kon inloggen op het 1GNC-intranet (vgl.

het digitale bankieren) en vanuit Nederland aan de oefening kon deelnemen. Het inloggen via het internet op het 1GNC-intranet gebeurt met een zgn. token die wachtwoorden genereert.

Het 1GNC-intranet is opgezet en beheerd door het Münster Detachement (MSDet) van het CISBn op het hoofdkwartier van 1 GNC (Hindenburgplatz (HBP), Münster (Duitsland)). Het is een netwerk in eigen beheer dat diverse CIS-diensten levert (zoals telefonie en e-mail) met een firewall die alleen geautoriseerde personen (met een token) vanuit het internet toelaat op het 1GNC-intranet. Overigens was het 1GNC-intranet al ruim voor de oefening Common Effort operationeel zodat militaire en civiele gebruikers al in aanloop naar de oefening via dit netwerk informatie met elkaar konden delen.



Figuur 1 - 1GNC intranet

CIS ONDERSTEUNING

Zo'n twee weken voor de start van de oefening (5 september) kwamen het Rapid CIS Element (RACE 7) van luitenant van Driel en de bataljonsstaf, ondersteund door het StafCoy, aan op de MvR-kazerne in Münster. Daarnaast stond het Münster detachement (MSDet) in het hoofdkwartier 1 GNC op de Hindenburgplatz klaar voor de ondersteuning van 1GNC-intranet. De taak was duidelijk; zorgdragen dat zowel TITAAN Mission Secret (MS) als 1GNC-intranet operationeel zijn vóór de opwarmperiode die startte op 14 september.

Hardware

Om de ondersteuning mogelijk te maken, is er een grote hoeveelheid aan CIS-middelen ingezet. Hierna volgt een overzicht van de ingezette middelen:

- MISSION SECRET (TITAAN)
  - circa 280 werkstations;
  - 235 Voice over IP toestellen (VoIP);
  - 25 printers;
  - 4 Video Teleconference (VTC) locaties;
  - 10x LAN Access Box;
  - 8x LAN Backbone Box.

- 1GNC Intranet
  - circa 300 werkstations;
  - 135 Civiel Analoge Toestellen (CAT);
  - 23 printers;
  - 66x COTS Switches;
  - 20 tokens voor het testen van de login via het internet.

Genoemde middelen zijn ingezet in zowel het afgeschermde als het open deel van de CP. Het afgeschermde deel bestond uit tenten en opleggers met werkruimte (OMW). Het open deel van de CP moest worden ingericht in één van de kantoorgebouwen op de kazerne. Verspreid over drie verdiepingen is hier het netwerk voor TITAAN MS aangelegd. Voor 1GNC-intranet was het mogelijk gebruik te maken van bestaande netwerkinfrastructuur van het gebouw. Wel heeft het RACE op grote schaal uitbreidingen aangelegd om alle gebruikers te voorzien van de benodigde werkplekken. Ook was het noodzakelijk delen van de bestaande netwerkinfrastructuur (switches en hubs) te vervangen door eigen apparatuur omdat de bestaande apparatuur defect was of niet paste in het netwerkarchitectuur.
Verder geldt binnen 1 GNC de Service to the Desk-procedure. Dat wil zeggen dat de eindapparatuur (zoals werkstation en het VoIP-toestel) klaar staan voor de gebruiker als deze binnenkomt. De gebruiker ontvangt van het RACE-personeel de gegevens die nodig zijn om van het systeem gebruik te maken en kan direct aan de slag. De End User Equipment zoals hierboven in het overzicht genoemd is op deze wijze aan de gebruikers aangeboden.

Services

De hardware leveren is één ding. Het gaat er uiteindelijk om dat de deelnemers hun werk kunnen doen en op een goede wijze de informatie kunnen uitwisselen met behulp van verschillende CIS-diensten (services).

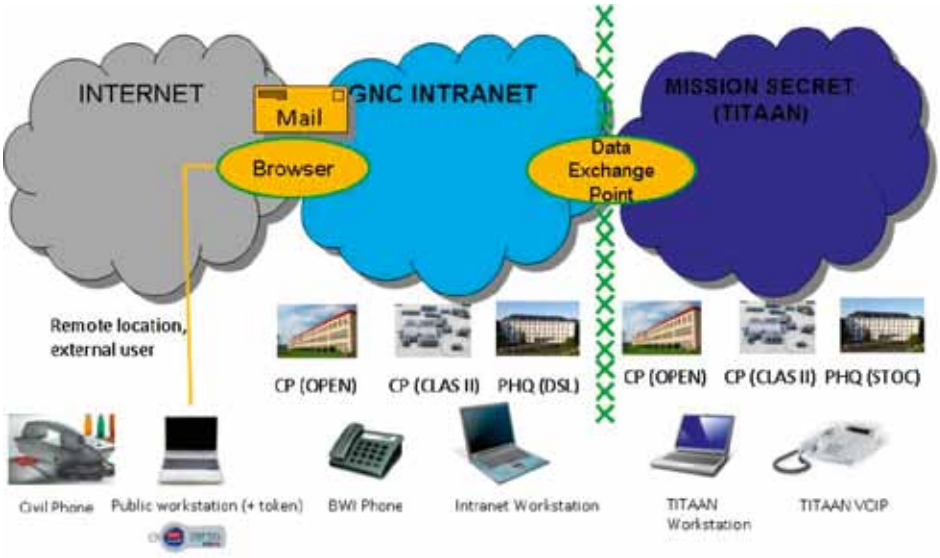
Voor het militaire TITAAN MS gaat het onder meer om file- and printer services (o.a. MS Office), telefonie (VoIP), e-mail (Outlook), C2IS (HEROS, de Duitse tegenhanger van ISIS) en videoteleconferencing (VTC). Via de Secure Voice Gateway (SVG) is het mogelijk om met de VoIP te bellen naar en gebeld te worden vanaf civiele telefoonnetwerken. Ook leverde het RACE een aantal specifieke toepassingen zoals bijvoorbeeld JCHAT (militair chatprogramma), JEMM (Joint Exercise Management Module), WISE (informatie portaal) en JOC-WATCH (een programma voor het Joint Operations Center waarop alle gebeurtenissen en incidenten in het operatiegebied worden bijgehouden).

Op 1GNC-intranet had men de beschikking over file- and printer services, telefonie (CAT), e-mail (Outlook) en een speciale WISE waarop alle deelnemende organisaties hun informatie konden plaatsen (zie ook figuur 2).

De beide netwerken waren fysiek gescheiden. Informatie delen gebeurde door tussenkomst van de gebruikers. Zo bepaalden TITAAN-gebruikers zelf welke militaire informatie op het 1GNC-intranet kon worden geplaatst. Verder waren voor zowel MS als 1GNC-intranet bijvoorbeeld zgn. content managers aanwezig die de informatie op de WISE-pagina's bijhielden. Het overzetten van bestanden tussen 1GNC-intranet en het TITAAN MS-netwerk gebeurde bij de Data Exchange Points. Daarbij maakte men onder meer gebruik van een scrubber; een laptop met open USB poorten en anti-virus software die anders is dan de standaard anti-virus software op het TITAAN MS netwerk. Daarmee werd voorkomen dat het TITAAN MS netwerk geïnfecteerd zou worden met een virus.

Wide Area Network (WAN)

Voor deze oefening namen er geen onder bevel gestelde eenheden van LCC deel en was de focus geheel op één locatie gericht. (zie figuur 3). Er is voor TITAAN MS dan ook maar één domein ingericht. Het WAN bleef beperkt tot een Line Encryption Unit (LEU)-verbinding met STOC (RACE 10 - Hindenburgplatz (HBP)) om onder meer



Figuur 2 - Netwerken binnen oefening Common Effort 11

de SVG (toegang tot het civiele telefoonnetwerk) te bereiken.
Voor 1GNC-intranet, dat werd beheerd door het MSDet op het Hoofdkwartier 1GNC op de Hindenburgplatz (Munster), werd het netwerk verlengd naar de oefenlocatie (MvR-kazerne) met behulp van een civiele 32Mbit/s point-to-point verbinding. Deze verbinding bleek één van de uitdagingen tijdens de oefening. Door een fout in de aanvraagprocedure van deze lijn was de apparatuur van de provider (T-systems) niet geleverd. De lijn was zogenaamd 'laag 2' (OSI model – Datalink layer) afgemonteerd in plaats van 'laag 3' (OSI model – Network layer). De provider was niet meer in staat om de benodigde apparatuur te leveren waardoor we zelf met een oplossing moesten komen. Nadat verschillende oplossingen zijn onderzocht is de beslissing genomen twee zgn. 'Pan Dacom'-modems aan te schaffen om de link operationeel te krijgen. Financieel bleek dit later een schot in de roos. De provider bood de eigen 'laag 3'-apparatuur aan voor een bedrag tussen de €10.000 en €20.000 terwijl de oplossing die nu was gevonden, slechts €1000 kostte.

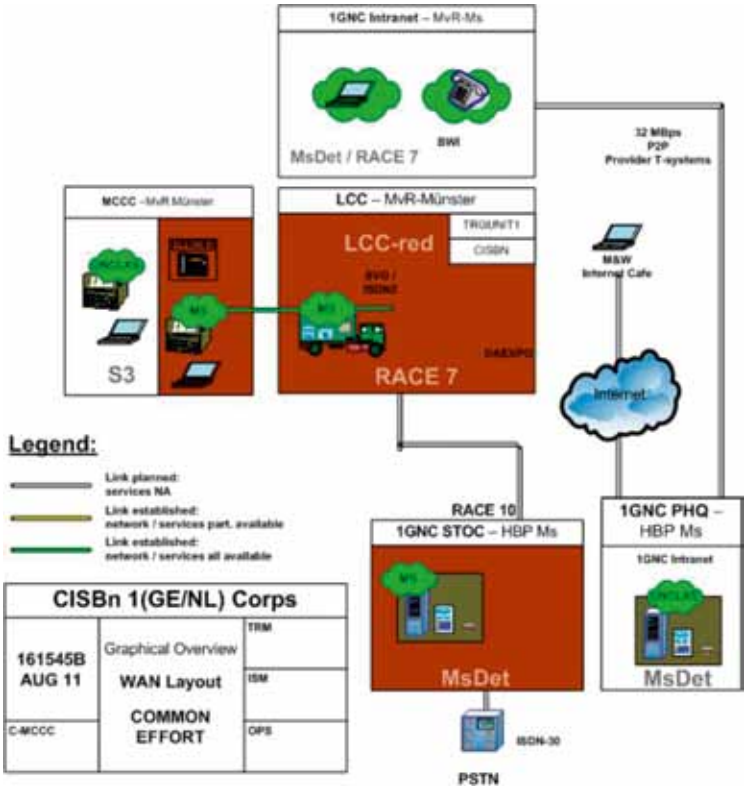
TOEKOMST

Common Effort was een bijzonder project waarbij de uitdaging vooral lag in de CIS-ondersteuning van de informatie-uitwisseling tussen 1 GNC en de civiele deelnemers op een voor ons nieuw netwerk, het 1GNC-intranet. Dit netwerk heeft op uitstekende wijze gefunctioneerd voor en tijdens de oefening. De ervaringen met 1GNC-intranet bij zowel de militaire als civiele gebruikers was positief. Het is eenvoudig te gebruiken en kent vele mogelijkheden om informatie met elkaar te delen. Die eenvoud is belangrijk omdat met name de civiele gebruikers uit verschillende delen van de wereld en uit verschillende organisaties afkomstig zijn.
Ook de koppeling van 1GNC-intranet met het internet (via een firewall) werkte prima. Deelnemers op andere locaties konden via het internet met een token eenvoudig inloggen op het 1GNC-intranet.

Zoals eerder vermeld, was het 1GNC-intranet al operationeel in de voorbereiding van de oefening en is dat nog steeds. Tijdens de oefening werd het netwerk slechts verlengd naar de oefenlocatie. Met 1GNC-intranet vervaagt het onderscheid tussen operationele netwerken specifiek voor oefening en inzet (o.a. TITAAN) en netwerken in vredestijd. 1GNC-intranet is één netwerk voor beide werelden.

Wel is gebleken dat de overheveling van informatie vanuit het geclassificeerde TITAAN MS-netwerk naar het 'open' 1GNC-intranet extra aandacht vergt. Deze overdracht geschiedt door de gebruiker en de kans bestaat dus dat geheime informatie via het 1GNC-intranet 'op straat' komt te liggen. Daar ligt dus een belangrijke rol bij de eigenaar van de informatie. Vooral in het begin was er binnen staf 1 GNC grote terughoudendheid om informatie op het 1GNC-intranet te publiceren. Dit veranderde naarmate men gewend raakte aan het nieuwe netwerk. Ook de civiele organisaties hadden in het begin schroom om hun informatie op het GNC-intranet te zetten, hoewel men er wel de noodzaak voor zag.

Het 1GNC-intranet was een experiment maar zal in de toekomst als service geleverd gaan worden om informatie met civiele organisaties en ministeries van landen uit te wisselen. De manier waarop het wordt aangeboden aan de militaire gebruikers zal naar verwachting wel worden veranderd. Op dit moment is het CISBn bezig met het ontwikkelen van een beheersbaar netwerk waarmee het stafpersoneel 1 GNC in het operatiegebied toegang krijgt tot het internet en daarmee ook tot het 1GNC-intranet. De naam voor dit netwerk is TITAAN WHITE. Door gebruik te maken van de al eerder genoemde token kan de militaire gebruiker (remote) inloggen op 1GNC-intranet dat op de Hindenburgplatz wordt beheerd. De eerste tests hiermee zijn al tijdens de oefening Common Effort gedaan en tijdens de oefening Odyssee Sword (november 2011) zal het voor het eerst zijn ingezet. Ik zal u dan ook, na de oefening Odyssee Sword, informeren over de inzet van het CISBn tijdens de oefening en in het bijzonder over de ontwikkelingen rond TITAAN WHITE.



Figuur 3 - WAN Overview