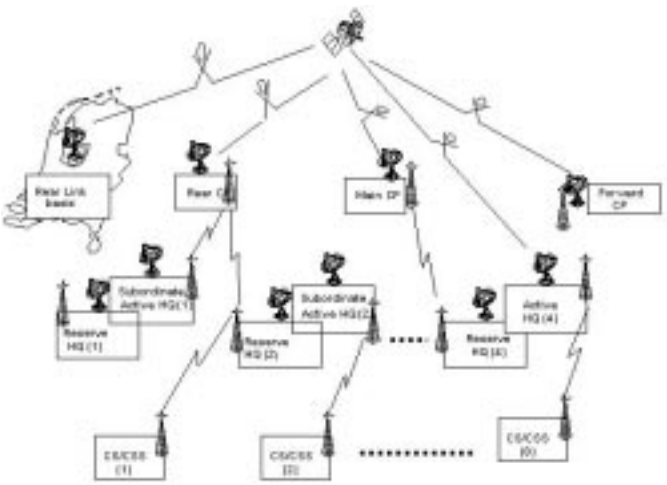
TITAAN: Flexibel en veelzijdig, maar ook veilig en betrouwbaar

Door: luitenant-kolonel (TS) A. Regtien, Projectmanager Titaan bij het C2SC / DM en
reserve luitenant-kolonel (LBJ) H.W. Evers, Senior Consultant bij Cap Gemini Ernst & Young

Het huidige verbindingssysteem van de Koninklijke Landmacht (KL), ZODIAC, voldoet niet langer om het optreden van de KL te ondersteunen. Bij inzet in (vredes)operaties moet de KL op dit moment vaak een ad hoc oplossing verzinnen. Daarom ontwikkelt de Koninklijke Landmacht, samen met de Koninklijke Luchtmacht, het Theatre Independent Tactical Army and Air Force Network, kortweg TITAAN. Dit uiterst flexibele verbindingssysteem vormt een slimme combinatie van militaire en civiele communicatie- en computerapparatuur, die overal ter wereld en onder alle omstandigheden bruikbaar is. In dit artikel willen wij u een beknopt overzicht geven van het beveiligingsconcept van TITAAN Fase 1 (voor het High Readiness Force Headquarters (Land), HRF(L) HQ) zoals dat nu ontwikkeld wordt door het Comnmand and Control Support Centre (C2SC).

OPZET TITAAN FASE 1

Het toekomstig operationeel optreden van HRF(L) HQ vereist flexibele en geïntegreerde communicatie- en informatie Systemen (CIS). Deze systemen moeten geschikt zijn om grote hoeveelheden spraak- en datacommunicatie te verwerken en het optreden over grote afstanden, in elk terrein, te ondersteunen. Tevens moet dit met zo weinig mogelijk CIS-personeel ter plaatse geschieden. Een apart datanetwerk (zoals TALANFA - Tactische LAN faciliteiten) uitrollen en beheren naast een conventioneel spraakgeoriënteerd netwerk (ZODIAC) volstaat daarom niet.

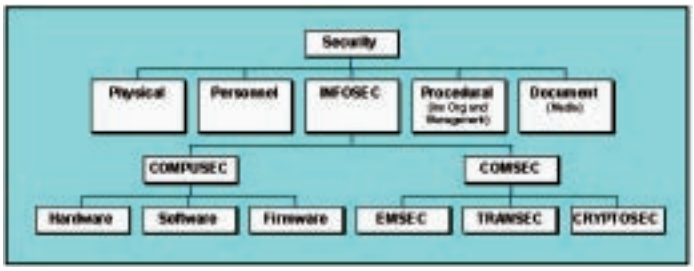


Figuur 1: Het Wide Area Network (WAN) van TITAAN

De basis voor TITAAN Fase 1 wordt gevormd door basismodulen (Local Area Netwerk - LAN), waarmee de commandoposten te velde van mobiele "kantooromgevingen" worden voorzien. Afhankelijk van te overbruggen afstanden, terreingesteldheid en andere operatie-afhankelijke factoren wordt een optimale combinatie van transmissiemiddelen ingezet om deze basismodules onderling te verbinden. Op deze wijze ontstaat een "Wide Area Network" (WAN - zie figuur 1). Vanwege het grotere afstandsbereik en de geschiktheid voor bergachtig terrein speelt satellietcommunicatie een primaire rol, naast straalzenders en eventueel ingehuurde landlijnen. Het netwerk wordt voorzien van de nodige beveiligingsvoorzieningen en moet aan andere, externe netwerken te koppelen zijn.

COMMUNICATIE- EN INFORMATIE SYSTEMEN (CIS) BEVEILIGING

In hedendaagse operaties is de beveiliging van CIS een cruciale factor. Immers, één van de pijlers van Network Centric Warfare is "Information Dominance". Het gevolg is dat CIS zich in meer dan normale belangstelling mag verheugen van allerlei organisaties en/of individuen die de informatie, welke zij ongeoorloofd kunnen verzamelen, tot hun eigen voordeel willen exploiteren. Dreigingen komen niet alleen van buitenaf, maar ook - en met name - van binnenuit. Niet altijd met voorbedachte rade maar meestal onbewust. Ze kunnen bijvoorbeeld het gevolg zijn van het "per ongeluk" wissen van gegevens, technische ongelukjes, etc..



Figuur 2: Overzicht CIS beveiliging

Een effectieve CIS beveiliging is een systeem van pluriforme, gebalanceerde maatregelen. Schematisch kan dit als volgt worden weergegeven (zie figuur 2):

DE BEVEILIGING BINNEN TITAAN FASE 1

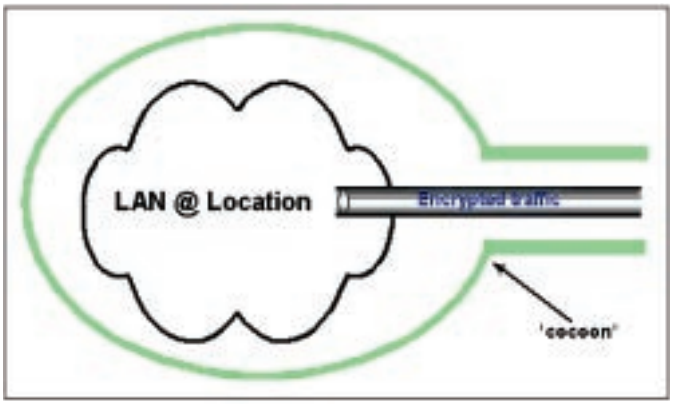
Voor TITAAN fase 1 is slechts weinig tijd beschikbaar: immers, juni 2002 moet de staf van 1(GE/NL)Corps (1GNC) reeds laten zien wat zij waard is. Zo moet rekening worden gehouden met de tijd die benodigd is om, naast het ontwerpen, ook het materiaal te bestellen en in te bouwen, het benodigde personeel te werven en op te leiden en de (beheer)organisatie aan te passen. De oorspronkelijke beveiligingsopzet van TITAAN is zeer geavanceerd en complex en was binnen die zeer korte tijd niet haalbaar. Er is daarom gezocht naar een oplossing die zonder verdere experimenten beschikbaar was en waarin bestaande naast nieuwe apparatuur kon worden gebruikt. Dit leidt er toe dat in het concept voor TITAAN fase 1 extra aandacht moet worden besteed aan andere (onderling samenhangende) delen welke niet door technologische maatregelen (kunnen) worden afgedekt. Het betreffen fysieke, organisatorische en procedurele maatregelen.

1 TALANFA: Tactische Local Area Netwerk Faciliteiten

Het streven binnen het C2SC is om zo pragmatisch mogelijk te blijven. Het communicatiesysteem moet immers blijven functioneren, ook onder moeilijke typisch militaire omstandigheden. Dit betekent dat tijdens het ontwerpen van TITAAN onder meer de volgende uitgangspunten zijn gehanteerd:

- als eerste prioriteit geldt dat het netwerk zonder al te veel problemen in bedrijf moet kunnen worden gesteld en maximaal operationeel te houden zijn en vanuit die optiek beheersbaar en te beheren zijn;
- vervolgens moet het - zoveel als mogelijk - de vereiste functionaliteit bieden;
- Tenslotte zorgen we dat het netwerk, binnen deze beperkingen, zo veilig mogelijk is.

Bovenstaande betekent dat het TITAAN-netwerk in fase 1 als basis een confidentieel netwerk lijkt. Echter, voor informatie met een hogere rubricering (bijvoorbeeld "Secret") zijn speciale, aanvullende regelingen getroffen; onder andere elektronische compartimentering gekoppeld aan specifieke procedurele, organisatorische en fysieke maatregelen.



Figuur 3: Het cocon model - LAN

Enigszins vereenvoudigd weergegeven is het beveiligingsconcept van TITAAN gebaseerd op de volgende drie elementen:

- het Cocon model;
- technische maatregelen en
- aanvullende fysieke, procedurele en organisatorische maatregelen.

Deze drie elementen kunnen als volgt worden beschreven.

HET COCON MODEL

Een commandopost (of delen ervan, zoals een cluster) zal zich altijd bevinden in een fysiek beveiligd gebied. Dit kan worden gezien als een (veilige) cocon met een LAN. In het TITAAN fase 1 concept zal al het dataverkeer dat deze cocon verlaat, worden vercijferd door middel van crypto. Schematisch kan dit model worden weergegeven als in figuur 3 is aangegeven. Worden alle "cocons" met elkaar verbonden in een netwerk, dan krijgt men een beveiligd WAN.

TECHNISCHE BEVEILIGINGSMAATREGELEN

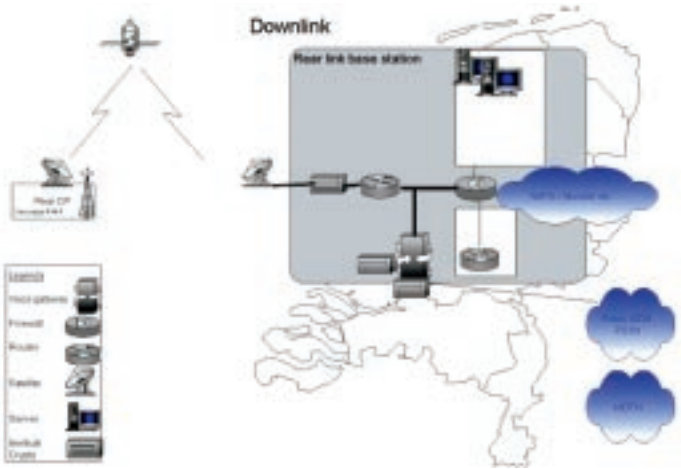
In fase 1 zal TITAAN deels gebruik maken van huidige componenten. Voor de FM200 straalzenderverbinding zal de vertrouwde Bundel Vercijfer- en Ontcijferaar - Mucolex (BVO-M) (zie afbeelding 1) gebruikt worden. Voor de beveiliging van het nog te verwerven interim-satcomsysteem zal nieuw, nog aan te schaffen, vercijferapparatuur zorgen omdat bestaande apparatuur binnen de KL of KLu niet in de gewenste bandbreedte kan voorzien. Getracht zal worden om één type vercijferapparatuur te verwerven dat, behalve voor interim-satcom, tevens geschikt is voor het vercijferen van landlijnen.

Afbeelding 1: De Bundel Vercijfer - Ontcijferaar - Mucolex (BVO-M)

Samengevat zullen de technische beveiligingsmaatregelen in fase 1 bestaan uit de volgende onderdelen:

- gebruik van vercijferapparatuur voor WAN verbindingen;
- firewall tussen het operationele domein en het statische domein;
- virusscanners;
- déactiveren van infra-rood ports, floppy drives, etc.;
- maximaal gebruik van de mogelijkheden van Windows 2000 zoals, bijvoorbeeld:
- gebruik van user-id en passwords als algemene toegangsbeveiliging;
- passwords om ongewenste booting tegen te gaan en
- screensavers welke met een password zijn beschermd.

De koppeling van het mobiele, operationele domein van HRF(L) HQ vanuit een buitenlands inzetgebied op het statische domein Duitsland/Nederland, ziet er schematisch als volgt uit (zie figuur 4).



Figuur 4: Koppeling mobiele op statische domein

FYSIEKE, PROCEDURELE EN ORGANISATORISCHE MAATREGELEN

Omdat binnen het ontwerp van TITAAN Fase 1 de technische maatregelen maar een relatief kleine rol kunnen spelen, is extra aandacht besteed aan aanvullende fysieke, organisatorische en procedurele maatregelen. Uitgangspunt hierbij is dat zo veel als mogelijk aansluiting wordt gezocht bij reeds bestaande richtlijnen. De basis van de additionele maatregelen is mede gebaseerd op zogenaamde "best practices". Hiervoor werkt het

C2SC nauw samen met o.a. het ECCM[1]-peloton en het NBV[2]. Vooral de ervaringen in recente vredesoperaties zoals in Bosnië vormen een dankbare bron van inspiratie.
Van elke categorie maatregelen volgen hieronder enkele voorbeelden. Behalve dat deze uiteraard niet volledig, noch limitatief zijn, is een strikte scheiding vaak niet mogelijk.

Fysieke beveiligingsmaatregelen
- gecontroleerde toegangsregelingen;
- bescherming van de locaties waar de gegevens / materiaal zal worden gebruikt;
- escorteren van niet-geautoriseerd personeel of bezoekers;
- toepassing van compartimentering. Het is onwaarschijnlijk dat al het personeel voldoende gescreend zal kunnen worden. Een speciale ruimte (voertuig) waar alle "gevoelige" informatie afgeleverd wordt en van waaruit het verder binnen de staf verspreid wordt moet dit aspect voorshands oplossen.

Procedurele beveiligingsmaatregelen
- het (vooraf) uitvoeren van veiligheidsonderzoeken (personen en materiaal!) en het - vervolgens - accrediteren;
- het opslaan en vernietigen van gerubriceerd materiaal;
- uitgifte van user-id en passwords;
- het beheren en behandelen van vercijfermateriaal en -apparatuur;
- meldingsprocedures aangaande veiligheidsincidenten.

Organisatorische beveiligingsmaatregelen
- delegatie van verantwoordelijkheden en bevoegdheden - denk hierbij aan bijvoorbeeld aan toezicht op naleving (handhaving);
- aangeven, structureren en inbedden van verantwoordelijkheden en bevoegdheden in de organisatie.

OVERIGE BEVEILIGINGSASPECTEN
Voor TITAAN fase 1 is een apart document ontworpen dat de beveiligingsregelingen voor deze fase van TITAAN meer in detail weergeeft. In dit document is, buiten de eerder aangegeven beveiligingsgebieden, ook plaats ingeruimd voor onderwerpen die op het gebied van CIS-beveiliging nadere richtlijnen behoeven.

- *Veiligheidsaspecten aangaande opslagmedia*

Behandeld worden onder meer zaken als de opslag, vernietiging (wissen), déclassificatie, herstel, reparatie en / of onderhoud. In een aparte bijlage wordt uitgelegd hoe de behandeling is van berichten welke een speciale afhandeling vereisen.

- *Specifieke veiligheidsmaatregelen met betrekking tot computers*
  In dit hoofdstuk wordt aangegeven welke veiligheidszaken van belang zijn als het gaat om hard- en software aspecten.

- *(Eventuele) Koppeling met andere netwerken en / of systemen*
  Behandeld worden - bij een eventuele noodzaak - de aandachtspunten van een koppeling met andere (bijvoorbeeld publieke) netwerken en welke veiligheidsaspecten hierbij een rol spelen.

- *Aandachtspunten betreffende het gebruik van portable apparatuur*
  Vanwege hun karakteristieken is het nodig dat voor portable devices (Palm-tops, electronische agenda's, e.d.) extra aandacht wordt besteed aan veiligheidsmaatregelen betreffende het medium, het gebruik ervan en de (opgeslagen) gegevens.

- *Rapportage van veiligheidsincidenten*
  Mochten zich veiligheidsincidenten voordoen is het van belang dat er een gestructureerde reactie op deze incidenten volgt.

EPILOOG
Een effectieve CIS beveiliging is een systeem van gebalanceerde, samenhangende maatregelen. Hoe die er voor TITAAN fase 1 uitziet is hiervoor beschreven. Maar het blijft uiteindelijk "mensenwerk" met de nodige risico's. Wellicht meer dan voorheen is "Information Security" (InfoSec) nu een verantwoordelijkheid - en daarmee een primair aandachtspunt - van de operationele commandant.

Beveiliging vraagt "offers" van gebruikers en "easy to use" mag niet verworden tot "easy to amuse". De noodzaak van een actief programma op veiligheidsgebied (bewust worden en handhaven) is van eminent belang. Want ook in het ICT-tijdperk geldt:

"Commandanten - let op Uw Saeck !"

1 ECCM Electronic Counter Counter Measurements
2 NBV Nationaal Bureau voor Verbindingsbeveiliging