Materieelbeheer Communicatie en Informatie Systemen

Jean Marie Nulmans

De kolonel van het vliegwezen stafbrevethouder Jean Marie Nulmans is sinds 2009 de chef van de sectie materieelbeheer Communicatie en Informatie Systemen van het directoraat-generaal *Material Resources*.

La gestion du matériel des systèmes de télécommunication et d'information (CIS) vise à offrir un environnement CIS de qualité, aussi bien en opérations à l'étranger que sur le territoire national. En particulier, cet environnement exige de porter une attention particulière à la continuité, à l'amélioration des performances, au suivi des évolutions technologiques, à la sécurité et l'autonomie opérationnelle, ce qui constitue le fil rouge des plans du gestionnaire du matériel. Pour la réalisation de ces plans, ce dernier cherche différentes solutions permettant d'acquérir ces systèmes de la manière la plus efficiente possible. La gestion du matériel ne se limite pas à l'acquisition et la gestion technique : la qualité des systèmes ne peut être assurée de façon durable que si une structure de support adaptée est également prévue.

Là où, jusqu'à présent, l'aspect financier jouait un rôle important dans les choix du gestionnaire de matériel CIS, la disponibilité des ressources humaines revêtira une importance croissante à l'avenir. L'outsourcing est souvent présenté comme la solution standard. Cependant, l'externalisation des activités engendre non seulement des frais supplémentaires, mais également la nécessité d'accorder une importance accrue à une gestion correcte de la connaissance et des compétences du personnel concerné. L'impact sur la future facture en personnel occupe donc une place de plus en plus centrale dans les actions prises aujourd'hui par le gestionnaire de matériel. Quand on regarde encore plus loin dans

l'avenir, une répartition interne judicieuse du personnel CIS de la Défense entre les différentes fonctions sera déterminante pour la qualité globale des systèmes de télécommunication et d'information.

De Communicatie en Informatie Systemen en hun vereisten

Elke organisatie is voor haar werking meer en meer afhankelijk van performante Communicatie en Informatiesystemen (CIS), zo ook Defensie.

Het materieel CIS van Defensie kan ingedeeld worden in twee grote families: de corporate CIS en de operationele C3-systemen *(Command, Control* en *Communication)*. De corporate CIS betreft de middelen waarmee de organisatie dagelijks kan functioneren. Dit omvat onder andere de ganse bureauticaomgeving en de grote beheerstoepassingen die draaien op ongeveer 20.000 pc's. De operationele C3-Systemen zijn de specifiek militaire systemen en toepassingen die ingezet worden in operaties en training voor het uitvoeren van de opdrachten van Defensie. Hier vindt men onder andere de militaire communicatiemiddelen met de klassieke radioverbindingen en de satellietcommunicaties alsook de ontplooibare netwerken en hun militaire toepassingen. De systemen voor luchtverkeersleiding en luchtverdediging zijn ook een deel van de operationele C3-Systemen.

Fig. 1: het militaire grondstation in Marche-en-Famenne verzekert de permanente verbindingen met de operatietheaters en de schepen.

Het is evident dat voor de operationele C3-systemen continuïteit primordiaal is. Gezien het grote aantal gebruikers van de corporate CIS, is het ook daar noodzakelijk dat de goede werking van de systemen bestendigd wordt. Wanneer bijvoorbeeld het logistieke beheerssysteem (ILIAS) onbeschikbaar is, betekent dit onmiddellijk dat de magazijniers geen stockbewegingen meer kunnen uitvoeren, dat onderhoudsactiviteiten niet meer kunnen geregistreerd worden en dat bestellingen en aankopen stilvallen. Deze continuïteit wordt verzekerd door robuuste systemen met voldoende redundantie en de invoering van de nodige procedures om tussen te komen wanneer dit nodig is.

De gebruikers verwachten ook optimale performanties van de verschillende systemen. Gezien de snelle technologische evoluties vergt dit een permanente opvolging van de werking en een continu streven naar verbetering. Vele systemen hebben een typische levensduur van vijf tot tien jaar en dienen in die periode nog de nodige updates te krijgen.

De toegang tot gegevens is ook niet meer beperkt tot de data in het eigen netwerk. Meer en meer wordt gebruik gemaakt van informatie die op het internet beschikbaar is en van toepassingen van partners zoals de toepassing voor het beheer van de transportvliegtuigen van het *European Air Transport Center*. Deze noodzaak tot interconnectie maakt de systemen kwetsbaar voor cyberincidenten. De beveiliging van de informatie en het vrijwaren van de werking van Defensie in deze context vergen dan ook de nodige inspanningen van de materieelbeheerders.

Voor de operationele systemen moeten de ingezette eenheden in staat zijn om autonoom hun opdracht uit te voeren en incidenten het hoofd te bieden. Dit maakt dat een aantal systemen in het theater beschikbaar moeten zijn zodat de ontplooide eenheid haar opdracht kan voortzetten, ook wanneer bijvoorbeeld de verbinding met België niet functioneert.

De acties van de materieelbeheerder om aan de vereisten tegemoet te komen

De verschillende vereisten van continuïteit, performantie en technologische evoluties, gecombineerd met een gepaste bescherming en de nodige operationele autonomie van onze CIS, worden concreet gerealiseerd op basis van een reeks projecten tegen een betaalbare prijs. Enkele voorbeelden:

Met het oog op de continuïteit, ook in het extreme geval van een calamiteit, werd het rekencentrum van Defensie ontdubbeld over twee gescheiden locaties en werd een *Disaster Recovery Plan* uitgewerkt waarbij de gegevens op beide locaties synchroon bijgehouden worden. Een volledige procedure voor het omschakelen tussen de locaties werd uitgewerkt en gevalideerd.

Om de performanties van het netwerk te verbeteren gaat Defensie over van het verouderde BEMILCOM gebaseerd op straalzenders naar een glasvezelnetwerk. Deze overgang heeft tot doel de capaciteit van de verbindingen te verhogen zodat de toepassingen van Defensie performant aangeboden worden aan alle eenheden. Daarnaast zullen de stabiliteit en beschikbaarheid aanzienlijk verbeteren en wordt het mogelijk om een aantal toepassingen verder te centraliseren waardoor de ondersteuning kan geoptimaliseerd worden.

Globale technologische evoluties dwingen de materieelbeheerders ook om bepaalde systemen te vervangen. Een algemeen gekend voorbeeld zijn de evoluties van de verschillende softwares, waarbij de ondersteuning voor oudere versies op een zeker ogenblik stopgezet wordt door de fabrikant. Dit probleem stelt zich ook voor bepaalde technologieën. Zo eindigt binnen afzienbare tijd de ondersteuning voor de klassieke telefoniesystemen en zal Defensie verplicht zijn om de overgang naar VoIP *(Voice over Internet Protocol)* te maken. Dit is dan ook gepland voor 2014-2015.

Om de veiligheid te verbeteren worden er acties genomen op het niveau van de werkstations en de netwerken. Alle lokale systemen in de kwartieren zullen gestandaardiseerd en onder centraal beheer gebracht worden, zodat een strikter toegangsbeheer tot het netwerk kan verzekerd worden. Dit zal in parallel met de overgang naar VoIP gebeuren.

Door deze toenemende cyberdreiging heeft ook de uitbouw van de geclassificeerde netwerken van Defensie aan belang gewonnen. Steeds meer groeit het bewustzijn dat het gebruiksgemak van bepaalde oplossingen niet opweegt tegen de risico's op informatielekken of onbeschikbaarheden. Territoriaal wordt het *Secure Defence Network* (SDN) uitgerold teneinde hiermee de nodige bescherming te bieden aan geclassificeerde gegevens. Dit SDN is eveneens gebaseerd op een centrale en ontdubbelde infrastructuur.

Alleen kan het SDN echter niet voldoen aan de specifieke vereisten van autonomie en continuïteit in operaties. Daarom wordt hiervoor een specifieke

ontplooibare oplossing uitgewerkt met lokale servers. Dit systeem heeft de naam *Mission Defence Network* (MDN) gekregen.

Fig. 2: de ontplooibare netwerken met hun servers, geïntegreerd in een shelter. Links staat de kern van het geclassificeerde ontplooide netwerk (MDN) en rechts de niet-geclassificeerde systemen.

Ook in het domein van de operationele communicatiesystemen worden de performanties verbeterd, onder andere door de aankoop in 2013 van drieëntwintig bijkomende satellietterminals. De redundantie van de satellietsystemen zal bijkomend verbeterd worden in 2014 door het koppelen van het Belgische en het Luxemburgse grondstation.

De totale kosten drukken door samenwerking

Naast de technologische uitdagingen blijft het ook noodzakelijk om binnen CIS de budgetten onder controle te houden. Iedereen wordt geconfronteerd met de beperkingen op bepaalde communicatiediensten en de dagelijkse

controles op het gebruik ervan. Dit is echter maar één aspect van de kostenbeheersing. Het is vooral door het zoeken naar schaalvergrotingen en samenwerkingsverbanden dat er geprobeerd wordt om de kosten van de systemen te beheersen. In het operationele domein zijn deze samenwerkingen in hoofdzaak internationaal, hetzij binationaal hetzij via de NAVO terwijl in het corporate domein zowel publiek-publieke als publiek-private samenwerkingen aan bod komen. Ook wordt de kost van de ondersteuning mee opgenomen in de bepaling van de totale kosten waardoor oplossingen zoals leasing wel interessant zijn.

In de operationele wereld zijn een aantal samenwerkingsverbanden uitgewerkt. Zo gebeurt de verwerving van het nieuwe luchtverdedigingssysteem in het globale NAVO-programma van *Air Command and Control System* (ACCS) en wordt de oplossing van EUROCONTROL bestudeerd als opvolger van ons nationaal SEROS II-luchtverkeersleidingssysteem.

Fig. 3: Het testen van de software van het *Air Command and Control System* (ACCS) is gestart.

Bilateraal onderhoudt CIS nauwe banden met Nederland en Luxemburg. Hierdoor beschikt Defensie over het gebruiksrecht van de Nederlandse *Land Command* en *Control-software* in ruil voor de inzet van vier Belgische

fulltime equivalenten aan de ontwikkeling hiervan. De samenwerking met Luxemburg in het domein van de satellietcommunicaties levert aanzienlijke besparingen op voor de Belgische Defensie doordat ons buurland de nodige bandbreedte ter beschikking stelt in ruil voor het delen van de nodige kennis en steun op dat vlak. Binnenkort zal het uitgebreide Belgische grondstation ook gekoppeld worden aan het nieuwe Luxemburgse grondstation om zo elkaars back-up te kunnen zijn.

Op nationaal vlak wordt in 2013 een akkoord geformaliseerd voor het gezamenlijke gebruik van één radar voor het leveren van de vereiste radardekking boven het militaire vliegveld van Florennes en het burgervliegveld van Charleroi. Hierbij vermijdt Defensie te moeten investeren in een nieuwe radar en worden de werkingskosten gedeeld met Belgocontrol.

Door het zoeken naar vernieuwende samenwerkingen wordt gestreefd naar kostenbesparingen. Een voorbeeld hiervan zijn de ruilovereenkomsten in het kader van het glasvezelnetwerk. Door de overcapaciteit op bepaalde trajecten te ruilen met publieke (gewesten) en private partners op basis van concessies worden grote investeringen vermeden en moeten de betrokken partijen instaan voor het onderhoud van kleinere trajecten zoals beschreven in artikel Publiek-publieke en publiek-private samenwerkingen in het kader van de upgrade van het *Wide Area Netwerk* van Defensie in editie 5 van december 2012.

De eindapparatuur waarmee de gebruiker dagelijks werkt dient ook continu mee te evolueren. Om de problemen van verouderde toestellen te vermijden en om de ondersteuning te optimaliseren werden leasingcontracten afgesloten voor de computers en printers. Voor de printers laat dat bovendien ook toe om telkens de nieuwste technologie in huis te halen, de herbevoorrading van de inkt ter plaatse te automatiseren en overtollige stocks te vermijden. De herstelcapaciteit van Defensie voor commerciële pc's werd gesloten (20 personen) en het contractuele *Service Level Agreement* (SLA) voor herstelling voorziet nu in een herstelling ter plaatse op de volgende werkdag. Dergelijke termijnen waren met een interne hersteldienst onmogelijk te realiseren.

De organisatie van de steun

De kwaliteit van de verschillende systemen wordt in grote mate bepaald door de steunstructuur die hiervoor in plaats gesteld wordt. Voor de corporate

systemen gebeurt de ondersteuning via de Territoriale Steun Structuur (TSS) met een organisatie in drie lagen. Bovenaan bevindt zich het Competentiecentrum waar 250 experten de centrale systemen onderhouden en de standaarden uitwerken voor de decentrale systemen. De tien *Regional System Support Centra* (RSSC's) zorgen in hun plateau voor de ondersteuning van de CIS-systemen. Een gemiddeld RSSC beschikt over vijftien personen voor het uitvoeren van opdrachten. Daarnaast heeft iedere eenheid een CIS Cel (CISC) voor de hulp aan de eindgebruikers. Hiervoor is één persoon per honderd gebruikers aangeduid.

De nationale Coordinator CIS TSS zorgt vanop de Defensiestaf voor de aansturing en begeleiding van deze structuur. De verbetering van de steun is gebaseerd op duidelijke instructies en procedures, een communicatie via de RSSC's tot bij de CISC's, een nauwgezette opvolging van alle incidenten en aanvragen en het geven van de nodige vormingen aan de betrokkenen. Door zowel systemen als werkmethodes te standaardiseren en maximaal te centraliseren wordt de TSS-structuur zo beperkt mogelijk gehouden. Dat deze werkwijze haar vruchten afwerpt, bewijst de zeer sterke verbetering van de tevredenheid van de eindgebruikers over de verkregen CIS-steun en het werk van hun CISC.

Voor de ondersteuning van de operationele systemen bestaat een gelijkaardige organisatie. De eenheden van de Landcomponent beschikken over NEC-teams *(Network Enabled Capabilities)* in iedere eenheid voor de autonome ondersteuning van de eindgebruikers. Daarnaast hebben de vliegbasissen en de CIS-groepen de capaciteit om de operationele C3-systemen te ontplooien (satellietterminals, netwerken, servers,…). De ontplooide systemen worden in een gevalideerde standaardconfiguratie ingezet. Deze worden gebouwd door het competentiecentrum. In totaal betreft de Ops CIS ondersteuning ongeveer 1400 functies.

De uitdaging van de toekomst voor de materieelbeheerder: de beschikbaarheid van het technische personeel

De algemene vermindering van technisch geschoold personeel laat zich ook steeds meer voelen binnen Defensie. De instroom van nieuw technisch personeel is niet meer in staat om de vertrekken op te vangen en er wordt dan ook verwacht dat de helft van de huidige CIS-functies tegen 2020 niet meer kunnen ingevuld worden. De hoofduitdaging wordt dan ook om, met de

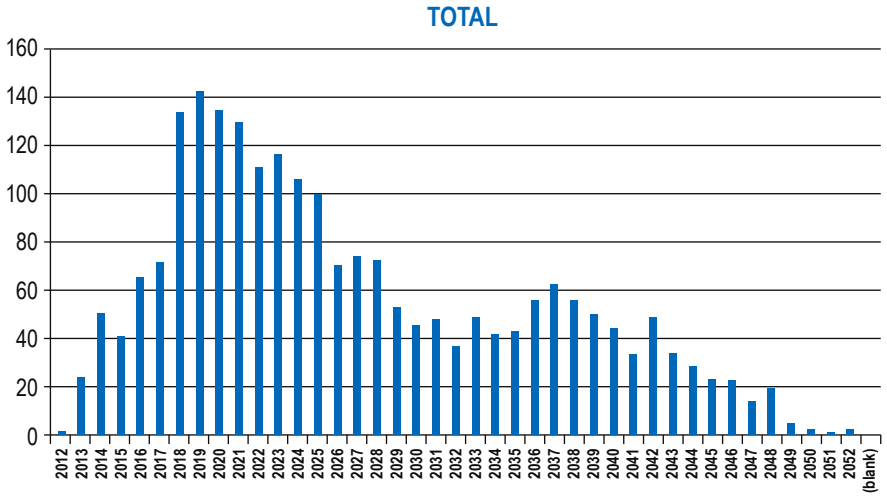

Fig. 4: De verdeling van het personeel op CIS-functies volgens het jaar van pensioen. De linkerkant toont de verwachte uitstroom terwijl rechts de beperkte instroom van de laatste 15 jaar te zien is.

beperkte budgettaire middelen, oplossingen te vinden waarbij met aanzienlijk minder personeel toch nog een degelijke dienstverlening kan geleverd worden.

Deze vermindering van het beschikbare CIS-personeel laat zich vandaag al voelen in de materieelbeheersplannen. Contracten die vroeger enkel gebruikt werden voor het verwerven van materieel worden nu uitgebreid teneinde ook designtaken en installaties te laten uitvoeren omdat het personeel ontbreekt om deze taken in-house uit te voeren. Zo worden bijvoorbeeld grote aanpassingen aan het centrale rekencentrum uitgevoerd door experten van burgerfirma's en werd een contract opgesteld voor het uitvoeren van bekabelingswerken.

Het is dan ook niet één enkele grote maatregel die een antwoord kan bieden aan deze evolutie, maar het zal een combinatie van allerlei maatregelen zijn waarmee ook in de toekomst kwaliteitsvolle CIS kan geleverd worden aan Defensie.

Vooreerst zal er moeten geïnvesteerd worden in de kennis van de mensen. De eerstelijnshulp aan de gebruiker die geleverd wordt door de CISC's en NEC-teams moet zodanig georganiseerd worden dat dit geen grote technische expertise vergt. Hierdoor kan een rekruteringsbasis binnen onze

organisatie ontstaan voor het invullen van deze doorstroomfuncties door ouder, niet-CIS-personeel met interesse in IT. Voor de experten moeten de nodige plannen en acties ontwikkeld worden om, ondanks het outsourcen van bepaalde taken, zich te verzekeren van het kennisbehoud binnen de organisatie. Dit is onontbeerlijk om de kosten en het niveau van outsourcing te kunnen beheersen.

Op technisch vlak moet een deel van de oplossing gezocht worden bij een doorgedreven standaardisatie en een maximale centralisatie om het rendement van de steun te kunnen verbeteren. Ook zal de steun van steeds meer systemen moeten uitbesteed worden. Door deze optie permanent mee te bekijken en open te staan voor allerlei samenwerkingsvormen moet er geprobeerd worden om dit zo economisch mogelijk te doen zonder de goede werking van de organisatie in het gedrang te brengen of de budgetten te doen exploderen.

Op organisatorisch vlak is het noodzakelijk om de verschillende systemen en configuraties in een globaal kader te beheren. In eerste instantie moeten de configuraties van alle systemen duidelijk vastgelegd en gedocumenteerd worden en daarna de toekomstige evoluties in een globaal plan passen. Sinds 2012 werd een specifieke functie netwerkarchitect gecreëerd om dit uit te werken.

Ook de veiligheidsaanpak kan niet overgelaten worden aan de individuele materieelbeheerders of experten die elk een fragment van het globale systeem behandelen. Teneinde tot een evenwichtige aanpak te komen werd één veiligheidsarchitect aangesteld die ervoor moet zorgen dat er een passend antwoord komt op de toenemende dreiging. Door een dergelijke globale aanpak vermijdt men de verspilling van resources aan niet-prioritaire maatregelen.

Desondanks zullen er ook een aantal fundamentele keuzes moeten gemaakt worden in verband met de omvang van de operationele steun en de verdeling van de human resources over de verschillende CIS-subcapaciteiten. Samen met de personeelsbeheerders is een studie gedaan die een realistische inschatting geeft van het beschikbare technische CIS-personeel in de toekomst. Deze studie moet leiden tot een meerjarenplan met de toewijzing van dit technisch CIS-personeel aan de verschillende CIS-subcapaciteiten. Pas wanneer een dergelijke toewijzing globaal aanvaard is, kunnen coherente materieel- en personeelsplannen opgesteld worden om een evenwichtige en kosteneffectieve CIS-dienstverlening te kunnen blijven leveren.

Conclusie

Het materieelbeheer CIS is dus niet alleen op technisch vlak een uitdagende functie om in een continu evoluerende omgeving op het juiste ogenblik de juiste technische keuzes te maken en zo aan de kernvereisten te blijven voldoen. Ook het zoeken naar creatieve oplossingen of nationale en internationale samenwerking maakt deel uit van de acties van de materieelbeheerder. Daarnaast vergt een goed materieelbeheer, naast een goede beheersing van de financiële kosten, ook een permanente bezorgdheid voor de kwaliteit en de beschikbaarheid van het personeel voor de ondersteuning van de verschillende systemen.

❐

Trefwoorden: CIS, materieelbeheer, technisch personeel