

# DOORONTWIKKELINGEN ICMS

Majoor L.Y.T. Brus, Staf CLAS Afdeling IV&CIS, G6, Nationale Operaties

Net als Defensie is de rest van de maatschappij steeds afhankelijker geworden van ICT-middelen om te kunnen functioneren, ook in het geval van een crisis. Maar juist in een dergelijke situatie is het niet altijd zeker of onze informatie- en telecommunicatiesystemen nog inzetbaar zijn, denk bijvoorbeeld aan een grote overstroming die gepaard zal gaan met het uitvallen van het elektriciteitsnetwerk. Het is dan ook nodig dat er een eigentijdse back-up faciliteit is. In dit artikel gaat majoor Lodewijk Brus, stafofficier Nationale Operaties, nader in op de doorontwikkeling van de TITAN basismodules Intensivering Civiel Militaire Samenwerking of kortweg ICMS die deel uitmaken van 101 CIS bataljon.

## HUIDIGE OPZET ICMS-DETACHEMENTEN

Defensie werkt al enige jaren samen met de civiele instanties als de veiligheidsregio's, provincies en gemeenten onder de noemer van ICMS (Intensivering Civiel Militaire Samenwerking). Hierbij worden defensiecapaciteiten gegarandeerd om ter beschikking gesteld te worden aan die civiele instanties. Het is een breed pakket van mensen en middelen, zoals een noodhospitaal, blushelikopter, genie-capaciteit, stafcapaciteit et cetera. Eén van die gegarandeerde capaciteiten is de back-up voorzieningen voor ondersteuning van bestuurlijke en operationele centra die in de volksmond bekend staat als de ICMS-detachementen.

In totaal zijn er drie detachementen, waarvan er één op 8 uur notice to move (NTM) staat en twee op 24 uur NTM. Deze detachementen worden geleverd door 101 CIS bataljon. Met een detachement kan op een willekeurige locatie in Nederland een LAN met server ontplooid worden, dat via een satellietverbinding gekoppeld wordt aan een WAN. Er zijn koppelingen met het telefoonnetwerk en met het internet. Een dergelijk detachement heeft zijn eigen energievoorziening en is daarmee onafhankelijk van de lokale elektriciteits- en telecommunicatievoorzieningen.

Wanneer er een uitval is van ICT-infrastructuur kan een detachement naast een bestuurlijk centrum (bijvoorbeeld een veiligheidsregio) ontplooiën. De staf van die veiligheidsregio beschikt dan over de basisvoorzieningen van een computer met MS-

## ICMS PELOTON 101 CIS BATALJON ONDERSTEUNT CIMIC OEFENING IN CENTRUM VAN ROTTERDAM

Rotterdam was het podium voor de oefening BORCULO. Volgens het scenario van de oefening was door een overstroming van de Maas geen voedsel en drinkwater meer voorhanden. Tevens lag de infrastructuur en het openbaar bestuur plat.

Het was de taak voor het CIMIC (Civiel Militaire Coöperatie) bataljon van de Koninklijke Landmacht om de Maasstad weer op de rails te krijgen. Van donderdag 11 tot en met zaterdag 13 oktober trokken de militairen in groepen van zes of zeven de stad in om op 22 verschillende locaties informatie te verzamelen die nodig was om de stad weer enigszins op orde te krijgen.

De operatie was bedoeld voor beroepsmilitairen en reservisten van het 1 CIMIC Bataljon uit Apeldoorn. In uitzendgebieden werkt het bataljon samen met hulporganisaties, plaatselijke autoriteiten en de lokale bevolking om het getroffen gebied weer op te bouwen. Dan kan door te helpen

bij het bouwen van scholen of bruggen, maar ook bij het herstel van de rechtsorde en het bestuur.

Aan de Parklaan werd een tentenkamp neergezet van waaruit de civiel-militaire operatie onder de naam Borculo werd geleid. Vanaf donderdag was er een module van het ICMS (Intensivering Civiel-Militaire Samenwerking) peloton van 101 CIS (Communicatie- en Informatie Systemen) bataljon op deze locatie aanwezig om het CIMIC bataljon te ondersteunen in hun CIS middelen. Zij voorzagen op deze locatie de commandopost met alternatieve werkplekken en vergaderruimtes van laptops, telefoons, printers en beamers.

Het ICMS peloton valt onder het 101 Communicatie en Informatie Systemen Bataljon te Garderen en heeft als taak om ten tijde van rampen of calamiteiten in Nederland een snelle inzet van netwerkfaciliteiten te garanderen. Een tweede groep, die standaard op 8 uur NTM staat, was donderdagnacht gealarmeerd om het CIMIC bataljon te kunnen voorzien van netwerkapparatuur en -ondersteuning op een vooruitgeschoven CP locatie.



ICMS rivieropstelling aan de Maas tijdens de oefening Borculo in Rotterdam

Office, een LAN, telefonie over IP en internet. Dit alles in een omgeving die zeer sterk lijkt op TITAAN, het framework waarop het ontwerp van de ICMS-detachementen gebaseerd is. Hiermee heeft die veiligheidsregio dan de regiovoering weer in eigen handen.

## LEREN VAN OPGEDANE ERVARINGEN

De ICMS-detachementen staan al een aantal jaren paraat. In die tijd hebben ze allerlei ondersteuning en oefeningen uitgevoerd. Uit de ervaringen van zowel de gebruikers als het ondersteunende personeel zijn een aantal punten naar voren gekomen:

- Voor de gebruiker is de aangeboden omgeving, gebaseerd op TITAAN, niet duidelijk.
- Er is een sterke behoefte om de data en programmatuur waarover de gebruiker in de normale situatie beschikt, te kunnen gebruiken.
- Het kost relatief veel tijd en is soms lastig om op een willekeurige locatie een LAN met kabels te kunnen ontplooiën.
- Er is behoefte aan de mogelijkheid om een VPN-verbinding te kunnen opzetten, om zo telewerken mogelijk te maken.
- Er is behoefte aan een koppeling met het Nationale Noodnet.

## TEKORTKOMINGEN

Het huidige concept voor de inrichting van de ICMS-BAMs stamt uit 2006. Toentertijd was er nog geen praktijkervaring met het ICMS-concept. Ook was toentertijd de stand van (internet) technologie minder ver gevorderd dan nu.

Uit verschillende oefeningen is een aantal zwakke punten van het huidige concept naar voren gekomen:

- In de huidige opzet is gekozen voor het werken in een bepaalde structuur, analoog aan de wijze waarop TITAAN is ingericht. Hierbij moet iedere gebruiker met zijn account inloggen op de server (BAM) en zijn aan die account een aantal zaken zoals e-mailadres, mappenstructuur etc. gekoppeld. In de praktijk is gebleken dat gebruikers moeite hebben om hiermee te werken. Dit komt omdat deze structuur niet op maat gemaakt is, maar volgens een generiek model. Het is immers van te voren onbekend waar een ICMS-BAM ingezet gaat worden en het aanmaken van een

Een aantal van deze punten is het directe gevolg van de keuze om de huidige architectuur te baseren op TITAAN. Zo is het van te voren onmogelijk te bepalen welke organisatie er ondersteund zal gaan worden. De inrichting van de informatievoorziening (User Provisioning List/Data) is dus zeer generiek opgezet. Hierdoor is maatwerk niet mogelijk en krijgt een gebruiker bijvoorbeeld een e-mailadres dat geen relatie heeft met zijn functie.

Het ICMS-compartiment vormt verder een eigen 'TITAAN-eilandje'. Er zijn wel koppelingen met het publieke telefoonnetwerk en het internet, maar omdat er nog altijd met TITAAN-werkstations binnen een TITAAN-LAN gewerkt wordt, zijn de mogelijkheden om andere dingen te doen dan bellen, tekstverwerken, een e-mail versturen of een internetpagina bekijken beperkt. Wanneer een gemeente elders een back-up locatie voor zijn netwerk opgezet heeft kan daar geen gebruik van worden gemaakt.

## EEN NIEUWE OPZET

Door de opgedane ervaringen te evalueren en dankzij nieuwe ontwikkelingen op het gebied van ICT is er een andere wijze van inrichten van de ICMS-detachementen voorzien. Hierbij draait de TITAAN-architectuur nog wel op de achtergrond, maar gaat het ICMS-detachement voor de gebruiker als een Internet Service Provider (ISP) functioneren. De gebruiker krijgt een gewone laptop en een aansluiting op het internet. Dit is voor hem een zeer bekende om-

specifieke structuur te veel tijd kost bij een plotselinge inzet.

- Ook al wordt een functionerende ICT-omgeving aangeboden, men beschikt niet over de data (gegevens) waarmee normaal gesproken gewerkt wordt. Deze data bevindt zich immers niet op de BAM. Het is ook niet mogelijk een eigen laptop op het systeem aan te sluiten waarop eventuele data zou kunnen staan. Ook is er maar een beperkt aantal applicaties (programma's) aanwezig op de BAM. Een specifieke applicatie die in gebruik is bij gemeente X kan dus niet gebruikt worden.

Het gevolg van bovengenoemde zwakke punten is dat Defensie een systeem aanbiedt dat eenmaal uitgerold niet helemaal aan de verwachtingen van de gebruikers voldoet. Tijdens oefeningen leidt dit vaak tot het blijven gebruiken van de organiek aanwezige systemen. Tijdens daadwerkelijke inzet kan dit leiden tot frustratie en een minder effectief gebruik van het systeem.

geving waarmee hij meteen aan de slag kan gaan. De telefoniefunctie blijft ongewijzigd.

De nieuwe opzet biedt een aantal mogelijkheden die de functionaliteit sterk verhogen:

- Er wordt een WIFI-netwerk uitgebracht. Hierdoor kan veel sneller ontplooid worden en zijn er ook minder belemmeringen door de infrastructuur van het gebouw.
- Het wordt toegestaan en mogelijk om eigen apparatuur aan te sluiten (Bring Your Own Device, BYOD). Zo kan programmatuur en data meteen weer gebruikt worden. Dit verhoogt de functionaliteit enorm.
- Het wordt mogelijk om een VPN-verbinding vanuit het ICMS-LAN te maken naar een eventuele back-up locatie.
- Er wordt niet meer met een vaste en generieke UPL-UPD gewerkt, maar gebruikersprofielen en e-mailadressen worden ter plaatse, aangepast aan de klant, gemaakt.
- Er wordt een koppeling naar het Nationale Noodnet opgezet.

Het resultaat is dus een meer open en flexibel systeem, dat de gebruikers veel meer mogelijkheden biedt en beter aansluit bij zijn verwachtingen. Hiervoor worden op het gebied van veiligheid een paar concessies gedaan. Zo brengt het laten aansluiten van eigen apparatuur natuurlijk onvermijdelijk risico's met zich mee. Het gaat erom bewust met deze risico's om te gaan en ter plaatse te beslissen wat verantwoord is.

## UITVOEREN VAN HET PLAN

Onlangs (september 2012) heeft het ministerie van Veiligheid en Justitie, dat de ICMS-detachementen financiert, toestemming gegeven om het voorgestelde verbeterplan uit te voeren. Voor eind 2012 moeten de ICMS-detachementen op de nieuwe manier ingericht zijn. Vanaf dat moment krijgt de klant, wie dat ook mag zijn, de beschikking over een flexibel en gebruikersvriendelijk systeem dat nog beter aansluit bij de behoeften anno 2012.

## SAMENVATTEND

Na vijf jaar ervaring met het optreden van de ICMS-BAMs en door nieuwe ontwikkelingen op het gebied van ICT is duidelijk geworden dat de huidige opzet van het systeem op eenvoudige wijze verbeterd kan worden. Door de generieke ICMS gebruikersindeling geheel te laten vervallen en in plaats daarvan eenvoudigweg internet aan te bieden binnen het LAN ontstaat er voor de gebruikers een veel transparantere werkomgeving. Ook biedt dit de mogelijkheid om



essentiële gegevens en software te gebruiken, die in de huidige opzet niet bereikbaar zijn.

In de nieuwe opzet wordt eigenlijk het hele TITAAAN-concept boven netwerkniveau niet meer gebruikt. Door allerlei veiligheidsbeperkingen is TITAAAN weliswaar robuust en informatieveilig, maar ook weinig flexibel. Voor de omgeving waarin de ICMS-BAMs ingezet worden is die flexibiliteit

echter zeer belangrijk en daarom moet er opnieuw nagedacht worden over de balans tussen veiligheid en functionaliteit, waarbij het opportuun lijkt om deze in de richting van functionaliteit te verschuiven.

Ook zijn er een aantal verdere verbeteringen mogelijk, al dan niet samenhangend met het loslaten van de generieke gebruikersindeling. Dit zijn het openstellen van het netwerk voor andere applicaties, het realiseren van

het LAN op WIFI-basis (draadloos), het opzetten van een website en het mogelijk maken van snelle uitbreiding van het aantal beschikbare BAMs. De traditionele en starre TITAAAN-structuur wordt deels losgelaten en vervangen door een meer flexibele en duidelijkere structuur die veel meer overeenkomt met de wijze waarop het internet is ingericht.

## AANDACHTSPUNTEN

Wanneer de ICMS-BAMs volgens bovenstaand concept ingericht gaan worden zijn er een aantal mogelijkheden en aandachtspunten die nog verdere uitwerking behoeven:

### Telefonie

Naast de functionaliteit van het computernetwerk is de functionaliteit (VOIP)-telefonie even belangrijk. Op dit moment wordt gebruik gemaakt van de callmanager, aanwezig op de lokale BAM, om telefonie mogelijk te maken. Omdat deze callmanager geconfigureerd moet zijn is dit systeem niet optimaal flexibel en al ook niet eenvoudig uit te breiden. Overwogen moet worden om de callmanagers op de HBS standaard te gebruiken en de callmanager op de BAM als fail-over in te richten.

### SharePoint

Er is al een test gehouden met web mail, deze was succesvol. Voor het gebruiken van een gedeelde netwerkomgeving is het mogelijk de applicatie SharePoint te gebruiken. Het functioneren van deze applicatie binnen TITAAAN moet nog onderzocht worden.

### Veiligheidsaspecten

Op dit moment is het niet toegestaan maar wel mogelijk om een eigen laptop op de ICMS-BAM aan te sluiten. Zoals al gezegd biedt het aansluiten van eigen apparaten veel mogelijkheden. Risico's hiervan zijn onder meer het binnenhalen van malware (virussen etc.) en het verstoren van de werking van de servers. Aangezien ICMS een domein (compartiment) is dat volledig losstaat van het operationele TITAAAN en in de nieuwe opzet (via de firewall) rechtstreeks gekoppeld is aan internet kan de afweging gemaakt worden tussen functionaliteit en veiligheid om niet-militaire eigen apparatuur toch aan te sluiten. Het risico kan – deels – ondervangen worden door een anti-virus-applicatie aan te bieden via de HBS. Ook mogen er niet zomaar applicaties geïnstalleerd worden op de gebruikte werkstations of op de BAM-server. Dit voorkomt

ook dat ongeautoriseerde software malware in het systeem brengt of dat deze in combinatie met aanwezige programmatuur het systeem laat crashen. Ook hier kan de afweging tussen functionaliteit en veiligheid opnieuw gemaakt worden.

### SDNO

Het Staf Detachement Nationale Operaties (SDNO) maakt ook gebruik van een ICMS-BAM voor zijn ICT-infrastructuur. Een essentieel verschil tussen deze werkwijze en die van de ICMS-BAMs in de ICMS-setting is dat de organisatiestructuur van het SDNO wel vaststaat en dat deze voor de gebruikers wel helder is. Ook worden er door het SDNO applicaties gebruikt die tot TITAAAN behoren, zoals ATHENA en ISIS. Iedere ICMS-BAM moet dus nog steeds de mogelijkheid hebben om als SDNO-BAM te functioneren. Ook moeten de werkstations nog steeds bruikbaar zijn binnen de SDNO-configuratie, waar ATHENA en ISIS als applicaties aanwezig moeten zijn.

### Back-up van informatie voor civiele actiecentra

Zoals vermeld is het met de nieuwe setting in principe mogelijk om remote in te loggen op de bedrijfservers van de te ondersteunen actiecentra. Hiervoor is het natuurlijk wel noodzakelijk dat een functionaris over de middelen hiervoor beschikt. Ook moet een dergelijk actiecentrum waarborgen dat er een server, die toegang biedt via de telestick, beschikbaar is. Als de primaire server in het rampgebied staat en dus uitgevallen is moet er uiteraard elders wel een back-up gerealiseerd zijn! Door deze nieuwe mogelijkheid onder de aandacht te brengen van het Ministerie van Binnenlandse Zaken wordt zij in positie gebracht een afweging maken om in een dergelijke back-up te investeren.

### Website

Een eenvoudige manier om de functionaliteit van de back-upvoorziening te vergroten is het opzetten van een website waarop actuele informatie te vinden is voor zowel de gebruikers van de voorziening als de buitenwereld (het internet). Denk hier bijvoorbeeld

aan een telefoonlijst met de nummers van de op de voorziening aangesloten gebruikers. Deze website zou opgezet kunnen worden met behulp van een Content Management System (CMS), waardoor deze op eenvoudige wijze beheerd kan worden door het personeel van de BAM. Overigens staat realisatie van een dergelijke website los van het aanpassen van de structuur. Op dit moment is het CMS-systeem WISE al opgenomen in de configuratie van de ICMS-BAM.

### WIFI

Op dit moment wordt het LAN uitgerold met behulp van kabels. Dit is een vrij tijdrovend proces en ook niet op iedere locatie even gemakkelijk te realiseren. Het is mogelijk om een LAN grotendeels draadloos te realiseren met behulp van WIFI. De benodigde investering hiervoor is heel gering en is van dezelfde orde grootte als de kosten aan het verknippen van kabels benodigd voor het enkele malen installeren van een LAN op kabelbasis. Er is op beperkte schaal getest of WIFI werkte binnen de ICMS-configuratie. Een uitgebreide test, met meerdere wireless access-points (WAP), moet nog plaatsvinden.

### Mogelijkheden tot uitbreiding

Defensie garandeert de inzet van 3 ICMS-BAMs. Deze staan dan ook altijd paraat voor inzet. De eenheid die de ICMS-BAMs in de bewapening heeft beschikt echter over een veel groter aantal BAMs; deze zijn echter geconfigureerd om ingezet te worden als netwerk voor militaire eenheden en kunnen niet op korte termijn omgezet worden tot ICMS-BAM. Er zijn echter scenario's denkbaar waarin dit zeer wenselijk zou zijn. Er zijn mogelijkheden om dit te realiseren tegen zeer lage kosten. Bij uitvoering zou dan een eerste –gegarandeerde– batch van 3 BAMs binnen de gestelde NTM van 24 uur beschikbaar komen en een eventuele tweede batch na bijvoorbeeld 48 uur.

### BRONNEN:

Commandant ICMS peloton 101 CIS bataljon elnt Anneloes de Geest



*ICMS Detachement 101 CIS bataljon aan de Maastijdens de oefening Borculo in Rotterdam*

## VEILIGHEIDSREGIO'S ONVOLDOENDE KLAAR VOOR UITVAL ICT/ELEKTRICITEIT

**Veiligheidsregio's zijn zich onvoldoende bewust van de mogelijke gevolgen van de uitval van ICT en elektriciteit. Continuïteitsplannen ontbreken vaak nog.**

Veiligheidsregio's zijn zich onvoldoende bewust van de mogelijke gevolgen van de uitval van ICT en elektriciteit. Continuïteitsplannen ontbreken vaak nog, blijkt uit een inventarisatie. Het risicobewustzijn moet omhoog, vindt minister Opstelten.

### C2000

Minister Opstelten heeft de Inspectie V en J onderzoek laten doen naar de storing die zich een jaar geleden voordeed in het telecomknooppunt in de Waalhaven in Rotterdam. Daarbij vielen allerlei cruciale verbindingen uit, waaronder die van C2000 (het communicatiesysteem van politie en brandweer) en het 112-systeem. Vier veiligheidsregio's ondervonden de gevolgen; brandmeldinstallaties werkten niet en delen van het Nationaal Noodnet vielen uit. De gevolgen vielen mee om dat het euvel zich 's nachts voordeed. KPN en de veiligheidsregio's hebben wel adequaat gereageerd, maar zouden toch veel beter voorbereid moeten zijn op dergelijke situaties.

### BESEF

Minister Opstelten meldt de Kamer dat de betreffende veiligheidsregio's zich wel bewust zijn van het belang van continuïteitsmanagement voor hun verzorgingsgebied, "maar dat zij zich slechts ten dele beseffen dat de uitval van communicatievoorzieningen zodanig grootschalig kan zijn, dat operationele hulpdiensten en andere vitale en/of maatschappelijke organisaties hun taken niet meer naar behoren kunnen uitvoeren." Drie van de vier regio's zijn wel bezig met het opstellen van continuïteitsplannen.

### PLAN

Opstelten heeft het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC) ook onderzoek laten doen naar dergelijke plannen bij organisaties in het openbaar bestuur en in de sector openbare orde en veiligheid (OOV). Tachtig procent van de organisaties in die sectoren had eind 2011 een continuïteitsplan voor uitval van ICT/elektriciteit moeten hebben, zo wilde het kabinet. Maar in werkelijkheid blijkt dat inmiddels nog maar 19 procent te zijn. Met de kanttekening dat ruim de helft het dit jaar wel voor elkaar wil krijgen. Gebrek aan tijd en capaciteit is de meest genoemde reden voor de ommissie.

### BEWUSTZIJN

Opstelten vindt dat het risicobewustzijn nog lang niet hoog genoeg is. Provincies en waterschappen nemen hun verantwoordelijkheid, maar gemeenten kunnen nog veel verbeteren. De grootste slag moet echter gemaakt worden door de politieregio's en - nog meer - de veiligheidsregio's. Die lasten moeten continuïteitsmanagement als belangrijk onderdeel van hun bedrijfsvoering zien, aldus Opstelten. Hij wil daarover in gesprek met het Veiligheidsberaad.

### ZEELAND

De Veiligheidsregio Zeeland stelt naar aanleiding van het onderzoek al over voldoende backup-systemen te beschikken om uitval van de standaard telefoonverbinding in crisissituaties te kunnen opvangen. De storing leidde destijds in Zeeland tot problemen met de communicatie tussen de meldkamer en de ziekenhuizen. Maar mobiele telefoon, mobilofoon, portofoon of het nationale noodnet bieden altijd uitkomst, aldus de VRZ.

### BRONNEN:

- <http://www.binnenlandsbestuur.nl/digitaal-besturen/>
- de heer Freek Blankena

