C2SC LEVERT BIJDRAGE AAN BRANDBESTRIJDINGSOEFENING

Luitenant-kolonel ing. Theo Sierksma, Hoofd Bureau Ontwerp & Bouw/Sectie Ontwikkeling C2SC

Het C2 Support Centre heeft in april 2010 een belangrijke rol gespeeld bij de ondersteuning van een bosbrandoefening van de Veiligheidsregio Gelderland-Midden. De kern hiervan was de toepassing van *ad hoc networking*, een concept dat is ontwikkeld door het C2SC om de (digitale) commandovoering te ondersteunen. Dit concept werd voor het eerst in september 2009 gedemonstreerd tijdens de oefening Combined Endeavor. Begin dit jaar werd het concept in Barcelona bekroond met een internationale *Innovation Award*. Met de succesvolle inzet van dit concept tijdens deze bosbrandoefening is wederom een belangrijke stap gezet in het aantonen van nut en noodzaak, gekoppeld aan een goede werking. Het is daarmee een stimulans voor de doorontwikkeling en het uiteindelijk beschikbaar komen van (commerciële) producten.

Bij natuurbrandbestrijding zijn mobiele datacommunicatie en digitale geografische kaarten met plotfaciliteiten onmisbaar in de hedendaagse commandovoering. Het belangrijkste knelpunt waar de brandweer (in analogie met de krijgsmacht) mee worstelt is, dat in grote natuurgebieden niet overal voldoende dekking is van (publieke) digitale netwerken om gegarandeerd informatie te kunnen uitwisselen. De brandweer in de regio Gelderland-Midden heeft daarvoor nu als nieuwe troef het genoemde concept.

Het huidige commandovoeringsysteem van de brandbestrijding maakt gebruik van publieke GSM-netten voor de gegevensoverdracht. Dat is direct de zwakke schakel, want deze netwerken hebben over het algemeen wel een goede dekking in stedelijke gebieden, maar in veel mindere mate in landelijke gebieden. In de uitgestrekte natuurgebieden van de Veluwe zijn er nogal wat plaatsen waar geen signaal is. De GSM-netten hebben slechts een beperkte capaciteit, onvoldoende voor het commandovoeringsysteem voor brandbestrijding. De volgende zwakke schakel ligt gelegen in het feit dat GSM en UMTS publieke netwerken zijn. Bij een calamiteit van enige omvang kunnen die netten overbelast raken, waardoor de hulpverleningsdiensten, die volledig afhankelijk zijn van de publieke infrastructuur, nog zeer moeizaam commandovoering kunnen doen.

De oplossing voor deze problematiek werd ontwikkeld in een zeer vruchtbaar samenwerkingsproject tussen Defensie en Veiligheidsregio Gelderland-Midden. Vanuit Defensie is geparticipeerd onder regie en funding van het innovatieproject i-Bridge van CDC/IVENT. Defensie participeert vanuit het besef dat ook zij voor haar tactische operaties behoefte heeft aan mobiele datatoepassingen in de meest uiteenlopende terreinomstandigheden. Defensie en Hulpverlening Gelderland-Midden vonden elkaar en het resultaat is een door DMO/C2SC gebouwd ad hoc routersysteem, dat in april 2010 onder operationele omstandigheden door de brandweer is beproefd en daarna operationeel in gebruik is genomen.

Alle betrokken brandweervoertuigen zijn hiervoor uitgerust met een mobiele ad hoc router voor WiFi. Dit onafhankelijke wireless LAN (Local Area Network) fungeert als drager voor de uitwisseling van informatie in het operationele Eagle-commandovoeringsysteem. Afhankelijk van terreinkenmerken en begroeiing bedraagt de afstand waarover eenheden contact met elkaar kunnen hebben ongeveer een halve kilometer tot maximaal drie kilometer. Een belangrijke voorwaarde is dat de WiFi-antennes 'zichtcontact' hebben met elkaar.

De eenheden kunnen zo lokaal informatie uitwisselen, maar daarmee is nog geen informatieoverdracht naar commandofaciliteiten buiten het brandterrein gewaarborgd. Om dat te realiseren zijn alle ad hoc-routers ook voorzien van een UMTS-modem. Alle dataverkeer naar nodes buiten het netwerk op de plaats incident verloopt via het publieke netwerk. Bovendien zijn twee terreinvoertuigen omgebouwd tot mobiel knooppunt. In geval van onbereikbaarheid, storingen of overbelasting van het UMTS-netwerk, wordt gebruik gemaakt van een satellietverbinding. Deze satellietverbindingen worden gedeeld door alle voertuigen van de via het ad hoc netwerk opererende eenheden.

Het project i-Bridge binnen Defensie maakt deel uit van het nationale innovatieprogramma voor veiligheid, waarin de overheid veel geld steekt. Dit project kan voor de krijgsmacht van grote betekenis zijn. Ook de krijgsmacht kan gebruik maken van een slim mobiel ad-hoc datanetwerk in gebieden met geen of weinig technische infrastructuur, bijvoorbeeld tijdens inzetmissies. De praktijkbeproeving tijdens de jaarlijkse natuurbrandbestrijdingsoefeningen in april is een toonbeeld van civiel-militaire samenwerking.

i-Bridge ad hoc router

COPI (Commando Plaats Incident) op de heide

Tijdens deze oefening waren vanuit zowel de Defensieorganisatie als de Veiligheidsregio Gelderland-Midden diverse VIP's uitgenodigd. Vanuit de Defensieorganisatie was dit genm Gijsbers (Hoofddirecteur Informatievoorziening en Organisatie, HDIO).
Reactie van HDIO na afloop van de oefening: "Prima resultaat op basis van innovatie". HDIO benadrukte ook nog: "Zeer verrassend resultaat gezien vandaag, maar om dit concept op de commerciële markt te krijgen is een bijdrage van alle aanwezigen nodig".

Het concept zoals dat nu operationeel is, is een zelfgebouwd prototype. Het prototype is gebouwd met bestaande *commercial-of-the-shelf* technologie. De oefeningen hebben aangetoond dat dit concept en prototypeconfiguratie duidelijk in een behoefte voorzien. Daarom is het zaak om een leverancier te vinden die het conform de opgestelde specificaties kan bouwen en op de markt kan brengen.

In de volgende uitgave van Intercom, zal een uitgebreider artikel verschijnen, waarin bovenstaand concept meer in (technisch) detail zal worden uitgelegd.

VIP's op de heide: genm Gijsbers (HDIO) en kol ir. Booman (C2SC)

GEKNIPT VOOR U .....

DURE RIJKSPAS NIET IN TREK

Zonder er ruchtbaarheid aan te geven is de uitrol van de Rijkspas opnieuw uitgesteld. De twee departementen die een begin hebben gemaakt met de implementatie, gebruiken de multifunctionele smartcard alleen als eenvoudige toegangspas. De aanschaf van de rijkspas kost de departementen 20 tot 25 miljoen euro. De implementatiekosten bedragen volgens deskundigen een veelvoud van dat bedrag.

INTERDEPARTEMENTALE SAMENWERKING

Een jaar geleden ontving toenmalig minister van Binnenlandse Zaken Guusje ter Horst de eerste Rijkspas. Bij die gelegenheid meldde ze aan de Tweede Kamer dat de multifunctionele toegangspas in april 2010 bij alle departementen in gebruik zou zijn. Begin dit jaar ging de programmamanager Rijkspas bij BZK ervan uit dat de kerndepartementen, op Defensie na, de pas 'na de zomer' in gebruik zouden hebben. Het streven is nu dat het eind van dit jaar zover is. De Rijkspas is een multifunctionele chipkaart die een ambtenaar niet alleen toegang biedt tot het eigen departement, maar ook een bezoek aan andere ministeries mogelijk maakt. Dankzij een extra contactchip kun je met de pas bovendien veilig inloggen op pc's en netwerken. De Rijkspas maakt interdepartementale samenwerking makkelijker en maakt tijd- en plaatsonafhankelijk werken mogelijk.

KETENTEST

Bij het Franse bedrijf Sagem liggen een half miljoen super beveiligde Rijkspassen klaar. Maar voor de ministeries de pas mogen bestellen, wordt het beheer van de brongegevens en de datacommunicatie uitgebreid getoetst door de AIVD en de Rijksauditdienst. Omdat veel departementen hun personeelsgegevens niet op orde hebben, komen ze niet door niet door die ketentest. Veel haast met het op orde brengen van hun brongegevens lijken de departementen niet te hebben. Tot nu toe hebben alleen het kleine ministerie van Algemene Zaken en het ministerie van Buitenlandse Zaken deze ketentests doorstaan. AZ heeft de Rijkpas begin dit jaar ingevoerd, maar gebruikt 'm alleen als toegangspas. Buitenlandse Zaken is begonnen met de uitrol op de Haagse locaties, maar de ambassades, consulaten en andere buitenposten zijn nog niet zover.

GEKRAAKT

De Rijkspas kampt al sinds de start van het project in februari 2007 met vertragingen. In maart 2008 bleek dat de contactloze chip die op de pas zou komen, de Mifare Classis, met eenvoudige software te kraken is. Op de pas die nu door Sagem wordt geleverd zit de Desfie-chip. Die is met de huidige technologie niet te kraken, stelt Kees van der Kaa, bij uitvoeringsorganisatie ICTU verantwoordelijk voor de ontwikkeling en implementatie van de Rijkspas. De prognoses van onderzoekers luiden dat een chip maximaal 4 tot 5 jaar meegaat. De Rijkspas heeft er dus al een kwart van z'n levensduur opzitten als de kaart eind dit jaar bij alle ministeries is ingevoerd.

BUSINESS CASE

Hoeveel het ontwikkelen en implementeren van de Rijkspas kost, wil het programmamanagement niet aangeven. De aanschaf van de 500.000 tot 600.000 passen gaat de ministeries in totaal 20 tot 25 miljoen euro kosten. Het op orde brengen van het databeheer, aanpassen van de ICT-infractructuur en het aanschaffen van toegangspoortjes en kaartlezers, kost volgens ingewijden een veelvoud van dat bedrag. Besparingen levert de invoering van de Rijkspas niet op. 'Er is geen business case', aldus ICTU-programmamanager Van der Kaa. 'Bij de Rijkspas gaat het niet over geld besparen, maar over makkelijk samenwerken op een veilige manier.'

WEINIG URGENTIE

Chris Verhoef, hoogleraar informatica bij de Vrije Universiteit, zet grote vraagtekens bij het dure Rijkspasproject. Bij beveiliging van gebouwen gaat het volgens hem niet om chips en encryptietechnieken. 'De lekken zitten meestal in het beheer van de data, de ingewikkelde software die je daarvoor nodig hebt of in menselijk gedrag.' En interdepartementale toegang lijkt geen hoge urgentie te hebben. 'Ik heb nooit gehoord dat er bij departementen enorme rijen staan te wachten om het gebouw in te kunnen.' Het ontbreken van een sluitende business case is een veeg teken', stelt de hoogleraar. 'Dat is bij IT-intensieve projecten een kritische succesfactor. Als je de baten van zo'n project niet kunt uitdrukken in geld, heb je zo weer een project dat miljoenen kost, maar niks oplevert.'

Uit: Binnenlands bestuur juni 2010
door Yvonne van de Meent