THEMA COLUMN: DRAADLOOS = VRIJHEID

De heer ir. Teus van der Plaat, IVENT Research en Innovatie Centrum

Op verzoek van de redactie is deze column in dit themanummer gewijd aan mijn visie op de draadloze toekomst. Daarnaast heb ik in mijn vorige column over de veiling van het commerciële frequentie spectrum (nummer 3 2012) beloofd in te gaan op de specifieke Defensiesituatie. Ik geef hierbij aan hoe de algemene ontwikkeling zal zijn, maar daarnaast geef ik ook mijn persoonlijke visie over hoe Defensie hierop zou moeten anticiperen. Met nadruk wil ik vermelden dat het hier in deze column niet gaat om officiële Defensiestandpunten, maar om de visie zoals we die bij het RIC in afgelopen tijd gevormd hebben naar aanleiding van ervaringen, onderzoeken, discussies met leveranciers van 4G software systemen, SIMkaart-leveranciers en met velen binnen en buiten de defensieorganisatie.

Waarom de titel Draadloos = Vrijheid ? Als ik aan mijn echtgenote vraag waar ze een hekel aan heeft is het draden door het huis. Ik denk dat ze niet de enige is. Bijna iedereen heeft een hekel aan draden. Draadloos heeft iets magisch. Er verplaatst zich iets wat je niet ziet, maar het is er wel. De mens kan zich overal bewegen en toch verbonden zijn. Dat appelleert aan het basale menselijke gevoel vrij te willen zijn van draden. Volgens mij is dat een van de belangrijkste succesfactoren van het fenomeen draadloos. Draadloos geeft Vrijheid.

FREQUENTIE SPECTRUM

Voordat we ook maar iets over draadloos gaan roepen moeten we even heel goed de situatie op het vlak van frequenties bespreken. Hier verwijs ik naar de vorige column waarin e.e.a. wordt uitgelegd. Het gaat hierbij om de spectrumverdeling voor commerciële providers, die bekend zal zijn op de publicatiedatum van dit nummer, maar nog niet bij het schrijven van deze column.
We onderscheiden drie soorten frequentiegebruik. Commerciële , licentievrije en special-interest frequenties.

• De commerciële frequenties, die voor een periode van 17 jaar, tot 2013, aan de mobiele operators verkocht zijn.
• De tweede categorie zijn licentievrije frequenties die iedereen mag gebruiken. Voorbeelden hiervan de bijvoorbeeld 27 Mc band, de Wi-Fi band in de 2,4 GHz en de 5 GHz en banden voor portofoonverkeer, draadloze microfoons en andere devices. Een zeer belangrijk onderdeel hiervan is de Dect Guard band die per 27 februari 2013 is uitgebreid van 3,5 MHz naar 5 MHz (2x) in de 1800 Mhz band en in Nederland voor iedereen vrij te gebruiken is tot vermogens van 0.2 Watt. Deze band bevindt zich in de commerciële 1800 MHz band waar naar verwachting 90% van de LTE devices in Nederland en Europa op zal kunnen werken.
• De derde categorie frequenties zijn de specifieke militaire frequenties die in NATO verband internationaal zijn vastgelegd. De trend in de laatste decennia is dat er een voortdurende druk is uit de commercie om militaire banden vrij te geven voor commercieel gebruik. De druk wordt zo groot dat Defensie al vele banden heeft moeten afstaan. Naar mijn verwachting zal deze druk niet kleiner worden, eerder groter, omdat er een explosie voorspeld wordt in het commercieel gebruik van draadloze technieken. Cisco voorspelt tot 2020 een factor 28 toename van het verkeer, en dit zal leiden tot een grote druk op extra frequentiespectrum. Met LTE is volgens de deskundigen bijna het theoretische maximum bereikt van het versturen van Bits door de lucht (Bits per MHz, theorema van Nyquist). Hoewel er nog wel enige verbetering is te verwachten is, is zeker dat dit geen factor 28 zal zijn. De enige mogelijkheid om meer capaciteit te verkrijgen is dan uitbreiding van het beschikbare spectrum, en deling van de cell-sites, ofwel hergebruik van de frequenties door kleinere cellen te maken. Vergelijk Wifi, waarbij ik rondom mijn huis binnen een straal van 15 meter wel 72 SSID's van Wifi telde. Hiermee is de Wifi band waarschijnlijk een van de meest efficiënt gebruikte banden ter wereld geworden.

FOCUS OP COMMERCIËLE DRAADLOZE COMMUNICATIE

Mijn stelling is dat Defensie zich steeds meer zal moeten richten op het gebruik van commerciële draadloze toepassingen. Hiervoor

zijn een aantal redenen. Allereerst de snelheid van de innovatieve ontwikkelingen. Elke maand worden er meer dan 50 nieuwe draadloze devices uitgebracht, terwijl het aantal specifieke militaire devices geschikt voor gebruik in militaire frequentie banden misschien minder dan 5 per jaar zal zijn. Sinds het begin van gestandaardiseerde commerciële (gsm) communicatie in 1992 zijn reeds 17.000 verschillende devices op de markt gekomen. Ik denk te kunnen zeggen dat er zeker een factor 100 meer commerciële dan de specifieke militaire devices uitgebracht zijn. Het gevolg hiervan is dat die prijs veel lager is en dat er in een groot tempoveel meer innovatie plaatsvindt in de commerciële wereld. Er zijn immers potentieel 6 miljard gebruikers die deze apparaten kopen en de omzet per jaar loopt in de triljarden euro's per jaar. Gezien de voorspellingen zal deze trend zich de komende tien jaar voorzetten en is het verwervingsproces zoals dat thans bij defensie geldt op geen enkele manier opgewassen tegen deze "tsunami" van steeds weer nieuwe devices met nieuwe toepassingen. Het kost Defensie vele jaren voordat er iets is gespecificeerd en verworven en op het moment dat het er dan is, is de techniek verouderd. Het roer moet dus wat mij betreft om. We moeten ons vooral focussen op het gebruik van commerciële apparatuur. Dit is goedkoper, innovatiever en technisch superieur.

DE SIM KAART IS CRUCIAAL

Alle 6 miljard gebruikers van commerciële draadloze apparatuur hebben een unieke identiteit en dus billing-relatie met een van de 700 commerciële operators ter wereld. Deze relatie komt via de SIMkaart al sinds 1992 tot stand, namelijk sinds de invoering van de eerste GSM telefoons. De SIMkaart en zijn security is uiterst belangrijk, want de grootste nachtmerrie voor een operator is dat iemand in staat is te gaan bellen via zijn draadloze netwerken zonder daarvoor te betalen. Er wordt dus al 20 jaar naarstig voor gezorgd dat dit systeem beveiligingstechnisch volledig dicht zit. Immers gaan er triljarden euro's per jaar door dit systeem heen, dus een hack heeft voor de operators in financiële opzicht dramatische gevolgen voor de operators. Deze SIMkaarten worden beheerd door speciale beveiligde card-management systemen, die via een voor gebruiker niet zichtbaar "onder water"-kanaalverbonden is met het SIM card-management systeem. Een gebruiker merkt hier in het algemeen niks van, maar een operator is met een commando in staat een SIM card te blokkeren of de data op de SIM kaart te wijzigen. Bijvoorbeeld het "voorkeursnetwerk" in het buitenland wordt door de operator via het SIM card-management systeem vercijferd veranderd zonder dat een gebruiker daar wat van merkt. Deze informatie wordt dan weggeschreven op de SIM kaart. Uitsluitend door de OPTA erkende operators kunnen SIMkaarten laten drukken. In Nederland zijn dat ongeveer 40 operators met een eigen draadloos netwerk (KPN, T-Mobile, Vodafone) en daarnaast ook zo genaamde MVNO's (Mobile virtual network operators) . Deze MVNO's hebben geen eigen netwerk , maar gebruiken een van de 3 fysieke radio netwerken door middel van een zo genaamde roaming agreement. Voorbeeld hiervan is Aldi Talk, Vast Mobiel, Lebara, Rabo mobiel, AH mobiel, Tele2, .. en nog vele anderen. Er zijn vele vormen van MVNO's. De meest verstrekkende vorm is degene die alles heeft behalve een eigen netwerk. Tele2 was hiervan een voorbeeld. (Tele2 heeft inmiddels ook een eigen 4G netwerk). Defensie beschikt samen met Pro-rail ook over een eigen mobiele netwerk code, als enige organisaties in Nederland die een Netwerkcode hebben terwijl ze niet de plicht hebben tot het uitrollen van een voor iedereen te benaderen netwerk (universele toegang) zoals alle andere bezitters van een Netwerkcode.
Bezitters van een netwerk code kunnen zelf SIMkaarten laten drukken door een aantal gespecialiseerde firma's . Per jaar worden er wereldwijd ongeveer 5 miljard SIM kaarten gedrukt en de kosten hiervoor zijn laag (enkele euro's per SIM kaart) .

BEVEILIGING SIMKAART

Zoals gesteld is de SIMkaart cruciaal in het hele draadloze verkeer, omdat elke SIMkaart wereldwijd een uniek adres (IMSI International Mobile Subcriber Identity) heeft en een billing-relatie met de eigenaar van een telefoon en de eigenaar van het IMSI-nummer. Onderzoek door het RIC heeft uitgewezen dat er vele mogelijkheden zijn om security op de SIM kaart te regelen.

Allereerst is er de mogelijkheid (over the air) de identiteit van de SIM kaart te wijzigen of aan te passen of uit te breiden. Sommige stukken worden 'hard coded' geprint op de kaart en kunnen niet veranderd worden, andere parameters wel. Het is ook mogelijk meer dan een identiteit (IMSI nummer) op een SIMkaart te zetten. Er zijn voorbeelden van firma's die SIMkaarten leveren met 24 verschillende identiteiten op een kaart. In elk land waar men naar toegaat een ander netwerk en een andere identiteit. Omdat defensie zelf een netwerk code heeft (204 22) kunnen we ook zelf IMSI nummers creeren en eigen SIMkaarten laten drukken. We kunnen vragen aan de Nederlandse operators of men bereid is naast de Defensie IMSI ook hun identiteit te zetten op de Defensie SIMkaart. Dit zal uiteraard altijd via een tenderprocedure moeten lopen, maar technisch is e.e.a. geen enkel probleem. Theoretisch zouden dus de identiteiten van alle

Nederlandse commerciële providers op de Defensie SIM kaart aangebracht kunnen worden. Uiteraard uitsluitend met toestemming en onder medewerking van deze providers. Vervolgens kan afgesproken worden wat het 'voorkeursnetwerk' is voor de Defensie gebruikers en welke de next best etc. De moderne telefoons en tablets zijn in staat om IMSI switching (het veranderen van identiteit) toe te passen. Afhankelijk van de veldsterkte besluit de telefoon over te schakelen op een ander netwerk. Als de Defensie netwerkcode is ontvangen zal de telefoon automatisch naar het defensienetwerk gaan, terwijl als er geen dekking is van een defensienetwerk de telefoon op de SIM kaart naar de alternatieve mogelijkheden zoekt. Iedereen kent dit fenomeen als men de grens over gaat. De telefoon schakelt dan automatisch over op een van de buitenlandse netwerken die aanwezig zijn en waar door de eigen operator een roaming agreement mee is afgesloten

GEBRUIK DEFENSIE NETWERK CODE

In dit scenario zou Defensie dus op die plaatsen waar geen commercieel netwerk aanwezig is, of waar men dat om redenen van prijsstelling of veiligheid niet wil gebruiken, zelf een netwerk kunnen aanleggen. Dit dient dan te gebeuren in de 'dect guard band' in Nederland en in het buitenland, nadat er een overeenkomst is met de daar actieve commerciële operators. Uiteraard zal zoiets in crisisomstandigheden anders gaan dan in vredes-oefenings-situatie. Echter in de "bewoonde "wereld is veelal een commercieel net beschikbaar, dus daar kan men gebruik maken van dit netwerk . Alleen in die situatie waar in dit opzicht zoiets beschikbaar is (op zee, in de Sahara etc.) zal men zelf een tijdelijk netwerk moeten oprichten. Door gebruik te maken van de Defensie netwerkcode kunnen daar alle commerciële apparaten gewoon werken.
De visie is dus, daar waar het kan gebruik te maken van commerciële netwerken, echter als het echt spannend wordt om operationele of beveiligingsredenen , wanneer de commerciële netwerken uitvallen, dan wel wanneer deze niet beschikbaar zijn moet Defensie zelf beschikken over apparatuur om binnen enkele minuten actief te kunnen worden.

TRAIN AS YOU FIGHT. FIGHT AS YOU TRAIN.

Omdat defensie dus in noodsituaties moet beschikken over eigen netwerkcapaciteiten is het handig en verstandig om ook op de "vredeslocaties" deze netwerken en deze netwerkcode te gebruiken. Naast financiële voordelen is dit ook gewenst, omdat blijkt dat zaken het best werken als er voor de manschappen geen verschil is in kantoor- en vechtsituaties.

KOSTEN VAN OP COMMERCIËLE STANDAARDEN GEBASEERDE NETWERKEN

In de negentiger jaren was de omvang van een netwerk core van een mobiel netwerk zeer groot. Een gehele computer vloer (200 vierkante meter) stond vol met kasten en apparatuur en er was sprake van grote hoeveelheden leveranciers-specifieke software en hardware. Echter ook hier heeft de Wet van Moore toegeslagen.
Zowel de kosten van de hardware als de software zijn enorm gedaald. De meeste software draait tegenwoordig op "gewone" Intel servers met Linux en er zijn thans reeds mobiele software cores op de markt die draaien op ARM processors met een vermogen van 2 watt. Deze toepassingen worden toegepast door Special Forces die de apparatuur in een 'rugtas' meenemen en dus overal ter wereld in zeer korte tijd voor bijvoorbeeld een tiental gebruikers een klein mobiel netwerk in de lucht kunnen brengen.

De kosten van de software zijn vergelijkbaar gedaald tot enkele duizenden Euro's voor een klein netwerk, terwijl een Defensiebreed netwerk voor minder dan een half miljoen euro software kosten genereert. Een ander voordeel is dat de nieuwe LTE 4G Core software volledig gestandaardiseerd is qua interfaces naar de hardware en software, waardoor bijna alle hardware (servers, radio systemen) volledig is gebaseerd op standaarden. Tientallen leveranciers leveren de zenders en antennes voor deze commerciële netwerken, die met elkaar gemixt kunnen worden, zodat er een grote concurrentie is met als gevolg steeds lagere prijzen voor de toe te passen hardware. De footprint van deze netwerken varieert dus binnen de standaarden van een tiental gebruikers tot vele miljoenen bij de grote operators. Voor 100.000 gebruikers is alle hardware onder te brengen in 1 19 inch kast.

EINDAPPARATUUR

Zoals gezegd komen er thans maandelijks meer dan 50 nieuwe devices uit, die gebruik maken van de commerciële frequentiebanden. De prijzen dalen en de technische mogelijkheden worden steeds groter. Technisch is het mogelijk deze apparatuur ook voor militaire frequentie banden dit soort apparatuur te maken, maar de kosten schieten dan omhoog, het gaat lang duren voordat e.e.a. beschikbaar is, dus in termen van innovatie lopen we dan per definitie weer achter op de commerciële markt, en dit terwijl de prijzen veel hoger zijn.
Een belangrijk aspect is de robuustheid van de commerciële apparatuur voor militaire toepassingen. Er heeft zich een complete secondaire industrie ontwikkeld die allerlei (waterdichte) hoesjes en hard plastic cases maakt voor de beschikbare apparatuur. Als er bij voorbeeld weer een nieuwe IPhone wordt aangekondigd stort deze industrie onmiddellijk zich op zo'n merk en men fabriceert een heel scala van accessoires. In het algemeen kosten deze accessoires niet veel en geven ze een redelijke tot goede bescherming . In het geval dat het apparaat uiteindelijk kapot gaat kan door uitwisseling van de SIM het apparaat in een mum van tijd vervangen worden door een reserve exem-

plaar. Dit is vaak goedkoper dan reparatie. Steeds meer worden het 'fire and forget' apparaten.

DRAADLOZE APPARATUUR VERVANGT DESKTOP

Door de grote processorkracht van de nieuwe smartphones, met quad core computer is de reken- en ook de geheugencapaciteit van die devices ruim voldoende om de thans in te voeren VDI defensie omgeving te draaien. Het beeld dat langzaam ontstaat is dat over enige tijd elke Defensie medewerker een Smartphone krijgt of zelf koopt, waarbij deze als veilige thuis werkplek gebruikt kan worden,op kantoor in een cradle gezet kan worden waarop een toetsenbord en beeldscherm is aangesloten en waarbij heel gemakkelijk de huidige VDI omgeving via de Telestick software gedraaid kan worden. Door het succes van de Telestick is deze software inmiddels wijd verspreid en gebruikt ongeveer 50% van al het personeel – burgers zowel als militairen - deze stick om veilig thuis te werken. Omdat de Telestick software ook kan draaien in een beveiligde omgeving op de smartphone en de identiteit van de SIM-kaart gehaald kan worden ontstaat hierbij de nieuwe werkplek van de toekomst.

Iedereen heeft een (zelf gekochte) of door defensie verstrekte smartphone. In deze smartphone zit een SIM die men van defensie krijgt. Op deze SIM zit ook een PKI certificaat zoals dat thans op de Defensie multifunctionele smartcard zit. Daarnaast bevat de SIM kaart de Defensie netwerkcode en daarnaast een of meer commercieel operator IMSI identiteiten. Het kan zo zijn dat men buiten de defensieterreinen belt met een door defensie te selecteren operator, maar zonder meer technisch uitvoerbaar is dat de defensiemedewerker zelf een contract sluit met een operator voor zijn privé gebruik. Het voert hier te ver alle opties uit te werken , maar er zijn zeer vele technische mogelijkheden. Elke mogelijkheid heeft zijn eigen financiële plaatje. De standaard blijft dat iedereen kan bellen zodra hij binnen het bereik is van een defensiecomplex . Omdat we dat kunnen doen via 4G LTE is de bandbreedte vanaf de telefoon of cradle naar het netwerk ruim voldoende om de huidige VDI datatransmissie over te doen. Uit metingen blijkt dat we bijvoorbeeld 500 concurrent Telestick gebruikers over een 10 MB verbinding kunnen servicen. Dat wil zeggen dat er dus per gebruiker voldoende bandbreedte is om een sessie te laten werken. Ook komende toepassing van video is geen probleem. Hierdoor kan veel van de huidige aanwezige LAN infrastructuur worden afgebroken. Al het verkeer kan immers draadloos verlopen. Om bescherming te hebben tegen EOV zal altijd wel een vaste (glas) infrastructuur aanwezig moeten zijn, maar zeker in vredesomstandigheden kan heel veel communicatie draadloos plaatsvinden. Als we deze toepassingen uitrollen op de vredeslocaties is de volgende stap deze ook te gaan uitrollen in stationaire militaire kampen, waarbij te denken valt aan als bijvoorbeeld aan iets als Kamp Holland in Afghanistan. De uitrol van zo'n netwerk is dan werk van uren in plaats van weken. Daarnaast is het heel flexibel, omdat meteen overal dekking is van het zelf meegebrachte draadloze LTE netwerk.

Omdat alle apparatuur ook op een accu kan draaien kan de communicatie gewoon doorgaan als toevallig gedurende enige tijd de stroom uitvalt. Ook de welfare voorzieningen zijn dan meteen aanwezig, immers men kan ook gebruik maken van een andere identiteit. De verbinding tusseneenheden op grote afstand en Nederland verloopt dan via een internetverbinding of via het MilSatcom systeem. In iedere situatie wordt dus gekeken welk communicatievehikel het beste en goedkoopste is. Gezien de nieuwe gecertificeerde crypto-apparatuur kan dit allemaal ook nog veilig gebeuren.

CONCLUSIE

In de blauwdruk van het nieuwe JIVC staat dat we enerzijds innovatief moeten zijn en anderzijds veel kosten moeten besparen. Verder geldt het adagium 'Goed is goed genoeg' . Het is mijn overtuiging dat door gebruikmaking van commerciële standaarden, commerciële apparatuur en frequenties de operatie van Defensie veel goedkoper en daarnaast veel sneller en innovatiever kan zijn. Uiteraard zal er altijd behoefte blijven aan echte Milspec apparatuur, maar omvang van die behoefte zal aanzienlijk kleiner kunnen zijn. Ik ben mij ervan bewust dat over deze visie er veel opmerkingen gemaakt kunnen worden, en dat zowel in positieve als in negatieve zin. Deze visie is vooral bedoeld om de discussie hierover binnen defensie en met de leveranciers van defensie te stimuleren, zodat we uiteindelijk een goede goedkope, innovatieve en betrouwbare voorziening kunnen krijgen.