TNO Informatie- en Communicatietechnologie

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek / Netherlands Organisation for Applied Scientific Research

Security
Brassersplein 2
Postbus 5050
2600 GB Delft

www.tno.nl

T 015 285 70 00
F 015 285 70 57
info-ict@tno.nl

TNO-rapport

34203

Security visie op Ambient Networks

Datum	22 december 2006
Auteur(s)	Drs.ing. D.J. Welfing, Dr.ir. P.J.M. Veugen
Review	Dr. J.M.E. Geers
Oplage	20
Aantal pagina's	49
Opdrachtgever	Doelfinanciering vanuit Ministerie van EZ, DGET

Inhoudsopgave

1 Inleiding

Dit rapport beschrijft de resultaten van het doelfinancieringsonderzoek "*Security visie op Ambient Networks*" dat TNO Informatie- en Communicatietechnologie voor het Directoraat-Generaal Energie en Telecommunicatie (DGET) van het ministerie van Economische Zaken (EZ) in 2006 heeft uitgevoerd. Het onderzoek geeft inzicht in de toekomstige kwesties (zeg over 10 jaar) rondom de kwetsbaarheden en dreigingen (dit noemen we de *security aspecten*) en de maatregelen die je hier tegen kunt nemen van Ambient Networks. Dit onderzoek doet aanbevelingen aan DGET voor het sturen op de beveiliging van de markt. Merk op dat dit onderzoek uitgevoerd is voor beleidsmakers, maar niet specifiek gericht is op nieuwe regulering op dit vlak.

De uitkomst van het onderzoek geeft DGET handvatten om eventueel te kunnen sturen op veilig gebruik van Ambient Networks in de toekomst.

1.1 Onderzoeksmethode

Door gebruik te maken van toekomstscenario's willen we inzicht krijgen in de security aspecten die (mogelijk) zouden kunnen gaan spelen binnen de toekomstige markt voor Ambient Networks om op basis hiervan beleidsaanbevelingen te kunnen doen. Binnen deze toekomstscenario's wordt zowel de vraag- als aanbodkant binnen deze markten getypeerd. Daarna worden voor elk scenario zowel op micro- (gebruiker), meso- (bedrijf of organisatie) als macroniveau (nationaal) de typerende eigenschappen beschreven. Vervolgens wordt globaal aangegeven wat de securityaspecten zijn van de (toekomstige) Ambient Networks. En daarna wordt voor elk scenario in beeld gebracht wat deze security aspecten per scenario betekenen en hoe hier mee om moet worden gegaan. Op basis van deze analyse (security visie) worden aanbevelingen richting DGET gedaan.

1.2 Leeswijzer

Dit eerste hoofdstuk biedt een inleiding op het onderzoek. In hoofdstuk 2 wordt uitgelegd wat onder Ambient Networks wordt verstaan en vervolgens wordt in hoofdstuk 3 kort de vraag- en aanbodkant binnen de toekomstige markt voor Ambient Networks geschetst. In hoofdstuk 4 wordt de toekomstige markt uitgebreider behandeld en worden vier mogelijke toekomstscenario's op micro-, meso- en macroniveau beschreven. Vervolgens worden in hoofdstuk 5 onder andere technische en algemene security aspecten genoemd waarvoor passende beveiligingsmaatregelen worden gegeven. Op basis hiervan wordt in hoofdstuk 6 per toekomstscenario een algemene beschouwing van een mogelijke beveiligingssituatie weergegeven waarna de eerder geschetste beveiligingsmaatregelen worden toegewezen aan de verschillende partijen in de markt, uiteraard per toekomstig marktscenario. En tot slot worden op basis hiervan, in hoofdstuk 7, de conclusies getrokken en de aanbevelingen gedaan.

1.3 Afbakening

Zoals gezegd gaat dit onderzoek over de security visie voor de toekomstige markt voor Ambient Networks. Dit onderzoek wordt voor wat betreft een aantal aspecten afgebakend:

- Er worden vier mogelijke scenario's voor de toekomstige markt voor Ambient Networks geschetst. Er zijn weliswaar vele scenario's mogelijk, echter hier wordt gekozen voor deze vier.
- Deze vier scenario's worden op drie economische niveaus beschreven (micro-, meso- en macro-economisch niveau).
- De markt (binnen de scenario's) wordt vanuit de vraag- en aanbodkant belicht.
- Voor wat betreft de security aspecten en de bijbehorende maatregelen wordt alleen ingegaan op de voor Ambient Networks typische kenmerken (snelle, dynamische en kortstondige communicatie). Er wordt hier niet gekeken naar de algemene dreigingen die uitgaan van de losse technieken.
- In dit onderzoek gaat het om de beschikbaarheid, integriteit en vertrouwelijkheid op netwerkniveau. Ook alle security aspecten die te maken hebben met het overschakelen van het ene naar het andere netwerk en het bewaken van de kwaliteit van de verbinding worden meegenomen. Om de complexiteit behapbaar te houden worden de diensten, die op de Ambient Networks worden aangeboden, buiten beschouwing gelaten.
- Daarnaast worden eventuele relevante omgevingsaspecten meegenomen.
- Tot slot wordt nog kort naar de gebruiker gekeken.

2 Wat zijn Ambient Networks?

“Ambient Networks” zijn de ICT-netwerken die horen bij de visie rondom “Ambient Intelligence” (AmI) [1]. Daarnaast is het ook de titel van het gelijknamige 6e kader project voor de EU (www.ambient-networks.org). Bij “Ambient Networks” kan *Ambient* ongeveer vertaald worden met ‘omgevend’ en *Networks* komt uiteraard overeen met ‘netwerken’. Feitelijk zijn Ambient Networks dus ‘de omgevende netwerken’, dat wil zeggen als een persoon op een zeker tijdstip zich op een zekere locatie bevindt, dan zijn de Ambient Networks de netwerken die zich in de (directe) omgeving van de persoon bevinden en waar hij gebruik van kan maken. Vanuit een gebruikersperspectief zien Ambient Networks er dan als volgt uit:

Figuur 2.1: Ambient Networks

De term “Ambient” (binnen de context van een toekomstige infrastructuur) is te zien als een vervolg op de term “Ubiquitous Networks”. Het verschil tussen deze beide benamingen is dat bij Ubiquitous Networks een gebruiker actief moet koppelen met de verschillende netwerken terwijl bij Ambient Networks een gebruiker naadloos overgaat op een ander netwerk als hij dit van tevoren heeft aangegeven te willen.

Ambient Networks gaat er dus over dat een gebruiker (in het midden van het plaatje) met verschillende middelen, binnen verschillende contexten, diensten afneemt waarbij hij potentieel een veelheid aan netwerken kan gebruiken. Deze diensten en netwerken worden op hun beurt weer aangeboden door verschillende aanbieders. In de volgende paragrafen wordt dieper ingegaan op de middelen, contexten en netwerken van Ambient Networks.

2.1 Middelen

Onder middelen wordt verstaan alles wat technisch nodig is om een dienst mogelijk te maken (uitgezonderd het netwerk zelf). Concreet komt dit neer op alle mobiele en stationaire apparaten (devices) die de gebruiker heeft en de applicaties die daarop draaien.

Figuur 2.2: Een gebruiker en enkele voorbeelden van zijn middelen

2.2 Contexten

De gebruiker kan een dienst gebruiken binnen verschillende contexten. Enkele voorbeelden van dergelijke contexten *kunnen* zijn:

- HAN - Home Area Network
- PAN - Personal Area Network
- BAN - Buddy Area Network[1]
- OAN - Office Area Network
- VAN - Vehicle Area Network
- ‘xAN’ … [enzovoorts…]

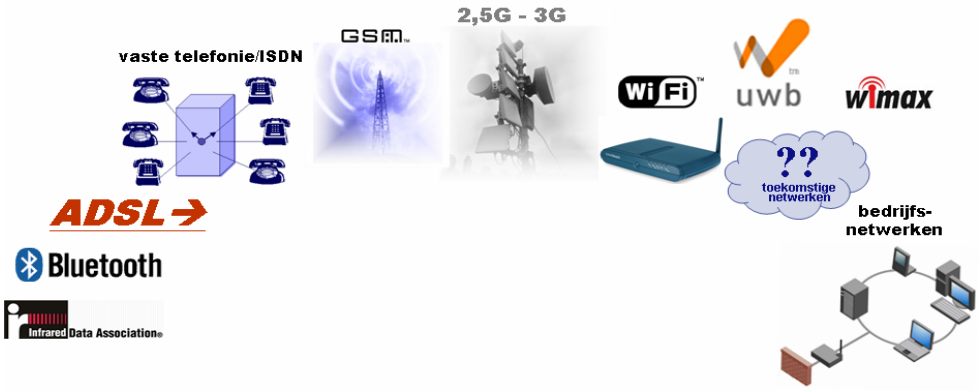
Kortom: er zijn oneindig veel ‘Area Networks’ mogelijk, waardoor de (toekomstige) contexten ook aan te geven zijn met de generieke term ‘xAN’.

Figuur 2.3: Enkele voorbeelden van mogelijke contexten

[1] Een Buddy Area Network (BAN) ontstaat wanneer personen (waarvan de vooraf afzonderlijk gedefinieerde profielen (opgeslagen in hun device) overeenkomstig zijn) bij elkaar in de buurt komen en via een draadloze korte-afstand-techniek (bijvoorbeeld Bluetooth) adhoc via hun device verbinding maken.

2.3 Netwerken

Deze netwerken en hun componenten zijn de daadwerkelijke ‘Ambient Networks’. De eerder genoemde middelen en contexten bewegen zich binnen deze Ambient Networks. Over deze verschillende bedrade en draadloze netwerken heen kan een gebruiker dan ook een dienst afnemen. Enkele voorbeelden van dergelijke netwerken zijn[2]:



Figuur 2.4: Enkele voorbeelden van Ambient Networks

- IrDA[3] (een verbinding door middel van infrarood licht)
- Bluetooth (een radioverbinding voor spraak en data op de korte afstand)
- ADSL[4] (breedbandig Internet)
- het vaste telefonienetwerk (ook wel PSTN/POTS[5]) en ISDN[6]
- 2G mobiele netwerk (ook wel GSM[7])
- 2,5G mobiele netwerk (ook wel GPRS of EDGE[8])
- 3G mobiele netwerk (ook wel UMTS[9])
- WiFi[10] (lokaal draadloos netwerk)
- UWB[11] (toekomstige zeer snelle korte afstand verbinding)
- WiMAX[12] (draadloos netwerk over grotere afstanden)
- vaste bedrijfsnetwerken

---

[2] Dit is niet een complete lijst. Denk bijvoorbeeld ook aan; DECT (Digital Enhanced Cordless Telecommunications, toegepast bij draadloze, analoge telefonie), adhoc netwerken, satelliet, ZigBee of VDSL (Very high Digital Subscriber Line, de opvolger van ADSL).
[3] Betreft de infrarode poort, onder andere toegepast op telefoons, PDA’s en laptops.
[4] ADSL staat voor “Asymmetric Digital Subscriber Line”.
[5] POTS staat voor “Publicly Operated Telephony System” of “Plain Old Telephony System”. PSTN staat voor “Public Switched Telephone Network”. Met beide wordt het ‘oude’ vaste telefonienetwerk bedoeld.
[6] ISDN staat voor “Integrated Services Digital Network” en is een vorm van digitale telefonie waarbij over de bestaande POTS-infrastructuur meer gegevens worden getransporteerd dan doorgaans met POTS zelf mogelijk is.
[7] GSM staat voor “Global System for Mobile Communications” (ook wel 2G).
[8] GPRS (General Packet Radio Service) is een uitbreiding op het bestaande GSM-netwerk en is bedoeld voor eenvoudig mobiel internetverkeer. EDGE vormt een uitbreiding op GPRS, staat voor “Enhanced Data Rates for GSM Evolution”, is een technologie voor datatransmissie en werkt op bestaande GSM-netwerken.
[9] UMTS staat voor “Universal Mobile Telecommunications System” en wordt beschouwd als de 3e generatie (3G) mobiele telefonie en is speciaal gericht op breedbandig mobiel internetten en o.a. de overdracht van videostreams.
[10] Wi-Fi staat voor “Wireless Fidelity” en is een certificatielabel voor draadloze datanetwerkproducten, die werken volgens de internationale standaard IEEE 802.11 voor draadloos Ethernet.
[11] UWB staat voor “Ultra Wideband” en is een nieuwe draadloze technologie, waarmee grote hoeveelheden gegevens bij hoge snelheden kan worden verzonden.
[12] WiMAX staat voor “Worldwide Interoperability for Microwave Access” en is de beoogde opvolger voor WiFi. WiMAX is nog niet op grote schaal operationeel.

3 De toekomstige markt

De toepassing van Ambient Networks vindt plaats in de toekomstige Nederlandse markt voor Ambient Networks. Deze markt kent een vraag- en een aanbodkant. En voordat überhaupt iets kan worden gezegd over hoe beleidsmakers om dienen te gaan met de toekomstige security aspecten van Ambient Network diensten, is het cruciaal dat men weet welke partijen opereren aan zowel de vraag- als de aanbodkant van de toekomstige Nederlandse markt voor Ambient Networks.

3.1 De vraagkant

De vraagkant van de markt bestaat uit de gebruiker die de op Ambient Networks gebaseerde diensten gebruikt. Deze gebruiker kan zich op micro-, meso- of macroniveau manifesteren als respectievelijk een individuele eindgebruiker, een bedrijf of een land.

3.2 De aanbodkant

Er zijn een aantal partijen te onderscheiden die op de aanbodkant van de toekomstige Nederlandse markt voor Ambient Networks zouden kunnen opereren. Deze partijen zijn over het algemeen op micro-, meso en macroniveau globaal dezelfde partijen:

1. Allereerst zijn er de huidige en toekomstige *netwerk operators* die speciaal voor telecommunicatie ingerichte netwerkinfrastructuren aanbieden. Dat kan zowel op lokaal als op nationaal niveau. Op lokaal niveau kan bijvoorbeeld een WiFi (of WiMAX)-netwerk worden aangeboden. Op nationaal niveau zijn dat op telefonie gerichte netwerken zoals vaste telefonie (PSTN) en mobiele telefonie (GSM), of de kabelnetwerken waar zowel TV, Internet als telefonie over kan worden aangeboden. Maar denk ook aan - speciaal voor mobiele telefoons en PDA's[13] - op dataverkeer gerichte netwerken, zoals GPRS en UMTS. Uiteraard geldt dat netwerk operators in de toekomst wellicht nieuwe protocollen gaan gebruiken voor toekomstige telecommunicatienetwerkinfra-structuren.
2. En dan zijn er de huidige en toekomstige *service providers*[14] die Internet toegang, e-mail, VoIP[15], IP-TV[16], location-based-services[17] en games aanbieden. Denk hierbij aan ADSL-aanbieders, kabelbedrijven (TV via de kabel) of VoIP-aanbieders, of mogelijk ook beheerders van applicaties.
3. En tot slot zijn er nog de *fabrikanten* die de hard- en software leveren voor de devices en infrastructuren.

[13] Een PDA, oorspronkelijk bedoeld als organiser of luxe elektronische agenda, is een zeer compacte 'hand-held PC' (waar tegenwoordig vaak ook al mee gebeld kan worden), waarbij PDA staat voor "Personal Digital Assistant".

[14] Het verschil tussen een netwerk operator en een service provider is dat een netwerk operator zich vaak richt op telefonie en netwerken met een landelijke dekking voor mobiele gebruikers (met mobiele devices zoals mobiele telefoons en PDA's), terwijl een service provider vaak Internet aanbiedt of zich richt op lokale datanetwerken.

[15] Voice over Internet Protocol ("bellen via Internet")

[16] Internet Protocol Televisie ("TV-kijken via Internet")

[17] Dit zijn diensten die gebruik maken van locatie-informatie van de locatie waar de gebruiker zich op dat moment bevindt. Bijvoorbeeld een dienst waarbij commentaar afgespeeld wordt op een PDA wanneer een gebruiker mee doet aan een rondleiding. (Waarbij het commentaar alleen wordt afgespeeld wanneer de gebruiker zich op een bepaalde plek bevindt.)

De overheid, niet deeluitmakend van de vraag- of aanbodkant, heeft hierin mogelijk een sturende en/of regulerende rol.

De toekomstige Nederlandse markt voor Ambient Networks is als ingewikkeld te typeren. Dit heeft een aantal redenen:

- *Veel verschillende partijen in de markt* - De toekomstige aanbieders die gezamenlijk het aanbod van Ambient Networks (diensten) aanbieden bestaan uit vele partijen die allemaal hun eigen rol hebben. Was het voorheen nog zo dat je als eindgebruiker één dienst van één partij afnam (bijvoorbeeld telefonie van de PTT) en met niemand verder iets te maken had, nu komen de rollen van al de spelers samen in een dienst die de gebruiker afneemt. Dat er nu zo veel partijen zijn, lijkt te komen doordat partijen zich specialiseren in een enkel aspect van de steeds complexer wordende diensten. Een gebruiker kan bijvoorbeeld bij een VoIP service provider een VoIP-dienst afnemen die Internet toegang gebruikt van een Internet service provider (ISP), waarbij de Internetverbinding wordt gerealiseerd over het netwerk van een netwerk operator heen. Door deze complexe opzet is het niet altijd duidelijk wie waar verantwoordelijk voor is binnen een beveiligingscontext.
- *Een partij kan meerdere rollen spelen* - Een netwerk operator kan bijvoorbeeld ook als service provider Internet aanbieden en hierop diensten aanbieden. Denk hierbij aan KPN die het ADSL-netwerk levert, daarbij een Internetdienst levert en vervolgens daar overheen een IP-TV-dienst aanbiedt.
- *De rollen van de verschillende partijen kunnen vervagen* - Service providers die lokale netwerken aanbieden en zich gaan verenigen, zodat ze landelijke dekking aanbieden, doen niet onder voor een landelijke netwerk operator. (Zo is het niet ondenkbaar dat lokale WiMAX-aanbieders mogelijk in de toekomst gaan samenwerken om een landelijk dekkend WiMAX-netwerk aan te bieden.)
- *Veel verschillende toekomstscenario's mogelijk* - Het blijft koffiedik kijken. Er zijn in de nabije toekomst vele scenario's mogelijk waarbij de hierboven geschetste redenen ook nog eens door elkaar heen kunnen lopen, wat ervoor zorgt dat de markt niet eenvoudiger wordt.

3.3 De vraag- en aanbodkant binnen een beveiligingscontext

Wat voor security aspecten spelen er bij de vraag- en aanbodkant op de markt voor Ambient Networks?

3.3.1 De vraagkant

Wanneer Ambient Networks, bekeken vanuit de vraagkant (de gebruiker), binnen een beveiligingscontext wordt geplaatst, dan betekent dit eigenlijk: "*dat een gebruiker met zijn middelen, binnen elke context, een dienst over de omgevende netwerken heen kan gebruiken zonder dat daar beveiligingsproblemen bij ontstaan*".

Een concreet **voorbeeld**:

- - - - - - - - - - - - - - - - - - -

Zo kan bijvoorbeeld, op microniveau, de eindgebruiker Thijs met zijn PDA vanuit zijn huis, auto of werkplek VoIP-bellen over plaatselijke WiFi- of 3G-netwerk heen zonder dat hij bloot staat aan beveiligingsrisico's (zoals een denial-of-service-aanval op zijn PDA of het WiFi-netwerk[18], of dat er op zijn kosten wordt gebeld[19] of dat zijn gesprek wordt afgeluisterd[20]).

[18] Een denial-of-service-aanval is een aanval (door een kwaadwillende) op de beschikbaarheid van de dienst.

- Thijs	(de gebruiker)
- PDA	(een middel van de gebruiker)
- huis, auto of werkplek	(drie contexten: HAN, VAN, OAN)
- VoIP-bellen over meerdere netwerken heen	(de Ambient Network dienst)
- WiFi- of 3G-netwerk	(twee ‘ambient’ netwerken)

- - - - - - - - - - - - - - - - - - -

3.3.2 De aanbodkant

Wanneer de toekomstige aanbodkant (de aanbieders) van Ambient Networks binnen een beveiligingscontext wordt geplaatst, geldt dat alle aanbieders zich bewust dienen te zijn van de beveiligingsrisico’s die men zelf loopt of die anderen (bijvoorbeeld de gebruikers) lopen. En uiteraard dient er ook naar gehandeld te worden. Op deze manier kan: “*een aanbieder met zijn middelen, binnen elke context, een dienst over de omgevende netwerken heen aanbieden zonder dat daar beveiligingsproblemen bij ontstaan*”.

Zo dienen de *netwerk operators*, die de netwerkinfrastructuren aanbieden, zich bewust te zijn van de risico’s die de implementatie en operationalisatie van dergelijke netwerken met zich meebrengt. Hun beheerproces dient hier op ingericht te zijn zodat de netwerken veilig te gebruiken zijn. En net zo moeten ook de *service providers*, die Ambient Networks diensten aanbieden, zich bewust zijn van de risico’s die deze diensten met zich meebrengen zodat de diensten op zich geen veiligheidsrisico’s kennen. En tot slot moeten ook de *fabrikanten* die de hard- en software leveren voor de middelen (devices en infrastructuren) op de hoogte zijn van de technische beveiligingsrisico’s en hiermee rekening houden bij het ontwerpen en produceren van hun producten zodat deze veilig zijn.

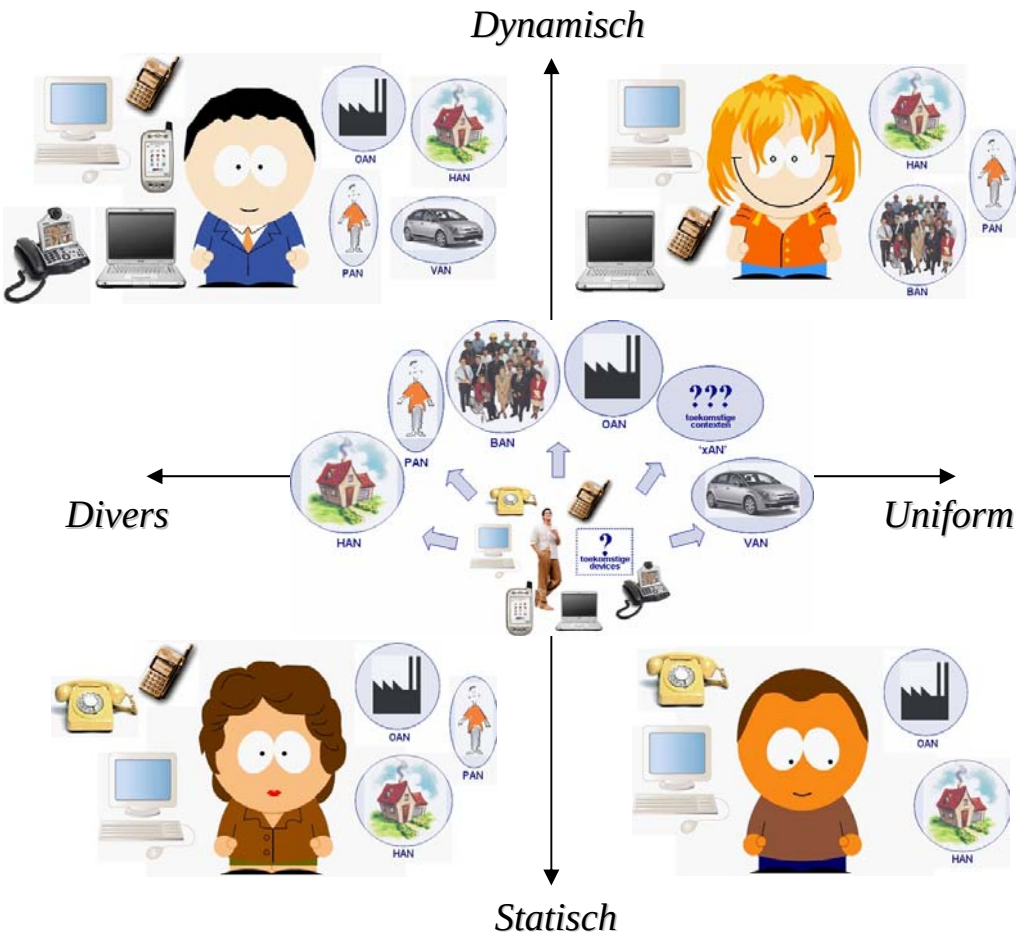
[19] Wanneer op Thijs zijn kosten wordt gebeld is de integriteit van de dienst in gevaar.
[20] Het afluisteren van een gesprek is een aanval op de vertrouwelijkheid van de dienst.

4 Scenario’s voor de toekomstige markt

Omdat Ambient Networks pas over een aantal jaren wellicht gemeengoed zijn en omdat we nu al een security visie willen geven, zal in kaart moeten worden gebracht hoe de vraag- en aanbodkant van de markt (uit Hoofdstuk 3) er dan uit ziet. Hiervoor worden scenario’s gebruikt.

4.1 De scenario’s - vraag en aanbod

TNO heeft bij eerdere toekomstverkenningen scenario’s ontwikkeld die voor de security visie in Ambient Networks opnieuw gebruikt kunnen worden [3]. Het gaat om vier scenario’s die over vier kwadranten worden verdeeld. De vier kwadranten ontstaan doordat twee assen elkaar kruisen, waarbij de assen de vraagkant en de aanbodkant in de toekomstige markt voor Ambient Networks voorstellen.



Figuur 4.1: Vier scenario’s voor Ambient Networks

In het midden van Figuur 4.1 bevinden zich de Ambient Networks en in elk kwadrant is een fictieve gebruiker afgebeeld met zijn of haar contexten en middelen.

4.2 Over de assen

In Figuur 4.1 is de vraag- en aanbodkant van en naar (de toekomstige diensten binnen) Ambient Networks weergegeven. Elk kwadrant staat voor een mogelijke toekomstige werkelijkheid van een omgeving die later in dit hoofdstuk op micro- meso en macro-economisch niveau wordt beschreven. De horizontale economie-as splitst de *aanbodkant* in de markt uit in de componenten “divers” en “uniform” en de verticale sociologie-as splitst de *vraagkant* (het gedrag van de gebruikers: het gebruik van en vraag naar de aangeboden diensten en netwerken) uit in de componenten “statisch” en “dynamisch”.

4.3 Over de as-uiteinden

- *Divers*: in een diverse markt zijn er veel verschillende aanbieders, elk met een zeer divers aanbod van producten en diensten.
- *Uniform*: bij een uniforme markt leveren de aanbieders (in het algemeen) een uniform aanbod en zijn er weinig verschillende aanbieders.
- *Dynamisch*: bij een dynamische vraag zijn mensen ondernemend, veel onderweg en de communicatie hierbij is kortstondig.
- *Statisch*: bij een statische vraag vertonen mensen passief gedrag, laten zich leiden en bevinden zich op vaste plekken, waarbij de communicatie langdurig is.

4.4 Kort over de kwadranten (scenario’s)

Op deze manier zijn de vier kwadranten te benoemen als vier scenario’s. Te weten:

- Scenario A: uniform aanbod, statische vraag ➔ **‘Afwachtend’**
- Scenario B: uniform aanbod, dynamische vraag ➔ **‘Bewogen’**
- Scenario C: divers aanbod, dynamische vraag ➔ **‘Complex’**
- Scenario D: divers aanbod, statische vraag ➔ **‘Degelijk’**

De scenario’s zijn als volgt kort te typeren[21]:

Scenario ‘Afwachtend’ *(uniform aanbod, statische vraag)*
“Hier gaat het om een samenleving die is gebaseerd op zekerheid. Er wordt wel bewogen, maar het komt steeds weer op hetzelfde uit. Hierdoor gaat innovatie niet zo snel. Grote bedrijven domineren de economie, waarbij een grote rol is weggelegd voor de EU, voor de publieke kant van de zaak. De consument zoekt comfort, vooral in het collectieve, bijvoorbeeld in zuilen en lidmaatschappen. Er zijn veel regels en aan traditie wordt veel waarde gehecht. In de gestructureerde samenleving overheerst functioneel denken. Hierdoor wordt er weinig verspild of over de balk gegooid. Zuinigheid is troef.”

Scenario ‘Bewogen’ *(uniform aanbod, dynamische vraag)*
“Hier gaat het om een krachtige, dynamische samenleving met veel activiteit en weinig keuze. Er wordt snel, kort maar krachtig gecommuniceerd. Bestuurders zijn als het ware krijgsheren. De staat reguleert milieunormen en diverse standaarden. Ook wordt het Aziatische model overgenomen om een vergelijkbare economie te verkrijgen. Er is economische groei. Er heerst veel activiteit waardoor veel wordt gereisd. Doordat de

[21] Deze paragraaf is tekstueel rechtstreeks overgenomen uit het eerder aangehaalde TNO-onderzoek [3]. De tekst voor de scenario’s A, B, C en D zijn overgenomen van respectievelijk de pagina’s 23, 15, 7 en 31 uit dit TNO-onderzoek.

samenleving efficiënt is ingericht, is er sprake van consolidatie. Er zijn weinig patenten. De ontwikkelingscyclus van producten en diensten is kort. Het is een trendy samenleving. Er vinden grootschalige innovaties plaats. De grote wens is dan ook dat Europa de meest innovatieve economie heeft."

Scenario 'Complex' *(divers aanbod, dynamische vraag)*
"Hier mag alles, kan alles én er gebeurt ook alles. Het is een individualistische interactieve samenleving die bruist van activiteit. Doordat er vele grote én kleine spelers in de markt zijn, is het product- en dienstaanbod complex en verre van transparant. Maatwerk is de maat. Hierdoor is ook de regelgeving per land en per regio zeer verschillend. Laat maar gebeuren. Nederland is te klein om producten en diensten aan te leveren, zodat de markt is geïnternationaliseerd. De economie zit op een hoogtepunt. De samenleving is in het algemeen welvarend, zij het dat er grote verschillen kunnen zijn. Het leven is een avontuur. Maar… vandaag een verliezer, morgen een winnaar. Het gaat immers om 'Survival of the fittest'."

Scenario 'Degelijk' *(divers aanbod, statische vraag)*
"De samenleving in scenario D is onthaast. Bedrijven zijn betrouwbaar. Mensen vinden 'cocooning' belangrijk, waarbij er thuis gerust wat kan worden geblowd. Ook economisch gaat het rustig aan, Nederland staat centraal en luxe komt naar je toe. In de consumenteneconomie is veel plaats voor vaste winkelformules (franchiseconcept). Diversiteit in aanbod komt uit het buitenland, voornamelijk uit China. De buyersmarkt is wel gericht op maatschappelijk verantwoordelijkheid. Antiglobalisering, Greenpeace en Alto staan centraal. Genieten mag en gebeurt ook, maar dan wel maatschappelijk bewust."

4.5 Uitgebreidere beschrijving van de vier scenario's

Nu de scenario's in de vorige paragraaf globaal zijn gekenmerkt, volgt hieronder een overzicht van de vier scenario's en hun uitgebreidere kenmerken. De bedoeling is om de verschillende scenario's te karakteriseren en de onderlinge verschillen te benadrukken. Hoewel niet bij alle aspecten direct de relatie met Ambient Networks zichtbaar is, wordt met de hele beschrijving wel een redelijk complete typering neergezet van een mogelijk scenario in de toekomst.

Per scenario worden vanuit de vraag- en aanbodkant vijf verschillende invalshoeken belicht. Allereerst op drie niveaus, namelijk op (1) micro-economisch niveau, vervolgens op (2) meso-economisch niveau en tot slot op (3) macro-economisch niveau [3]. Concreet betekent dit dat op microniveau gekeken wordt naar een individu, op mesoniveau naar een bedrijf(stak) en op macroniveau naar een land. En dat steeds voor zowel de vraag- als de aanbodkant van de toekomstige markt binnen het scenario. Tot slot wordt kort gekeken naar (4) de technologie en (5) de trends binnen elk scenario.

4.5.1 Scenario 'Afwachtend' (uniform aanbod, statische vraag)

Scenario A is algemeen samen te vatten in de woorden: globalisering; standaardisatie; zekerheid; grote rol EU; langzame productcycli; langzame innovatie; veel structuur voor wonen en werken; functioneel denken, weinig frivoliteit; grote bedrijven domineren de economie; collectief is belangrijk; aan traditie wordt veel waarde gehecht; weinig immigratie; '9 tot 5'; achteruitleunende consument zoekt comfort; stacaravan in de duinen; conservatief; verzuiling / lidmaatschap; minder grote welvaartverschillen; stagnerende economie; bezuinigingen.

4.5.1.1 Op microniveau - Arend

Bij scenario A hoort het individu Arend:

- Gebruiker **Arend**[22] (werknemer bij een klein administratiebedrijf);
- heeft de middelen: vaste telefoon, computer;
- heeft de contexten: HAN, OAN;
- gebruikt de netwerken: een bedrijfsnetwerk en het vaste telefonienetwerk;
- gebruikt de diensten: ‘vast’ bellen en e-mailen.

Figuur 4.2: Arend (werknemer bij een lokaal administratiebedrijf)

Vraagkant: Arend (42) fietst elke werkdag naar zijn werk en heeft een administratieve functie bij een lokaal administratiebedrijf. Voor zijn werk belt hij een aantal keren met zijn naaste collega’s en zijn contacten buiten de organisatie. Op het moment dat Arend vanuit zijn OAN naar buiten belt, wordt het spraakverkeer over het interne bedrijfsnetwerk gestuurd waarna het naar buiten toe geschakeld wordt over het digitale VoIP telefoonnetwerk. Na een lange werkdag komt hij thuis en komt tot rust: geen computers meer! Thuis heeft hij namelijk geen computer. Wel heeft hij een, middels een speciale adapter op het landelijke VoIP-netwerk aangesloten ouderwetse bakelieten draaischijftelefoon (dat is een hobby van hem), waarmee hij wekelijks met zijn familie belt. Arend gebruikt geen op Ambient Networks gebaseerde diensten.

Aanbodkant: Het bedrijf van Arend is beperkt, alleen wanneer er niet aan te ontkomen was, overgestapt op ‘nieuwe’ technologie. Het liefst zou het bedrijf de oude vertrouwde telefooncentrale weer gebruiken, maar het is tegenwoordig ‘VoIP’ wat de klok slaat.

4.5.1.2 Op mesoniveau - het bedrijf van Arend

Vraagkant: Het administratiebedrijf waar Arend werkt kent een hiërarchische structuur waarbinnen status en traditie telt. Het bedrijf is procesgericht, kent een lage concurrentie en een lage servicegraad c.q. dienstverlening. Er heerst een sterke ‘9 tot 5’-mentaliteit en mensen werken vaak gedurende een langere periode bij deze organisatie. Het bedrijf wil in grote hoeveelheden produceren, kent een lage innovatiegraad en doet

[22] Arend, Bianca, Constantijn en Deborah zijn getekend met behulp van ‘South Park Studio’ (http://www.sp-studio.de).

weinig investeringen. Enkele bedrijven die ook voldoen aan deze omschrijving zijn de NS, Shell, Ohra, Nuon, Essent en De Rekenkamer [3, blz. 26].

Aanbodkant: Arends bedrijf kent weinig diensten waarbij gebruik gemaakt wordt van Ambient Networks. Er is wel een LAN (Local Area Network) waar alle computers aan hangen. Dit is niet draadloos uitgevoerd en in dit zelfde netwerk zijn de vaste (VoIP)telefoons gekoppeld. Er zijn (vrijwel) geen diensten die over meerdere netwerken heen lopen. Of het moet belverkeer zijn wat op het interne bedrijfsnetwerk op basis van IP wordt getransporteerd en eventueel naar buiten wordt omgezet naar PSTN (analoog, circuitgeschakeld) verkeer.

4.5.1.3 Op macroniveau - het Nederland van Arend

Vraagkant: Het Nederland van Arend is te typeren als een land wat innoveert wanneer de EU dat verlangt. De economie stagneert en kent een lage groei. Er zijn minder politieke partijen dan anno 2006. Het land kent veel regels (tot op de millimeter). Men streeft naar rust en reinheid (rijtjeshuis). De inwoners gaan weinig op reis (eventueel wel vier weken op vakantie naar Frankrijk). Men houdt van naar de bioscoop gaan, bingo, dansles, sjoelen, bridgen en het KRO-programma “Toen was geluk nog heel gewoon”. Het ambacht is weer belangrijk [3, blz. 27].

Aanbodkant: Er zijn wereldwijd weinig aan Ambient Networks gerelateerde diensten beschikbaar. In Nederland worden dan ook weinig nieuwe netwerken opgetuigd. Daar is ook weinig behoefte aan. En wanneer Ambient Networks internationaal operationeel zijn, worden deze tot in detail dichtgetimmerd met regels en protocollen waarin is vastgelegd wie welke diensten hoe mag afnemen op welke netwerken.

4.5.1.4 De technologie binnen scenario ‘Afwachtend’

De algemene technologie binnen dit scenario is als volgt te typeren [3, blz. 28]: mensen kijken nog steeds TV, maar men heeft een DVD-recorder in plaats van een videorecorder (feitelijk neemt men nog steeds dezelfde diensten af, maar men maakt wel gebruik van nieuwe technologie). Er is weinig multimediale dienstverlening en beeldcommunicatie en men gebruikt Internet, met een vaste desktop-PC, op een passieve manier (vooral voor surfen en e-mail). Er is weinig draadloze techniek, wel maakt men gebruik van ‘mobiliteit’ op het vaste netwerk (WiFi-accesspoints op vaste punten binnen een bedrijf). De landelijke overheid verlengt de GSM-licentie en er is geen drang naar ‘moderne’ draadloze technieken zoals WiMAX en UWB. In Europa zijn er vier centrale mobiele operators die mobiel bellen aanbieden. De focus binnen deze grote markt ligt op goedkoop bellen en internetten.

4.5.1.5 De trends binnen scenario ‘Afwachtend’

De algemene trends binnen scenario A zijn:

Europa

1. Leven wordt geregeld vanuit Brussel;
2. Er is sprake van Europees protectionisme;
3. Er is weinig innovatie.

Internet for Everything

4. Internet wordt wel gebruikt voor zoeken van informatie en voor e-mail;
5. En niet tot weinig voor real-time communicatie (men gaat bijvoorbeeld nog steeds naar gemeentehuis voor het regelen van zaken).

Vergrijzing

6. In dit scenario is sprake van enig conservatisme en gemeenschapszin;

7. Er is veel behoefte aan zorg en een grote druk op jongeren om in verzorging te werken.

Globalisering

8. Het economische en culturele leven gaat meer-en-meer langs de mensen heen.

Verschuiving economische macht naar Azië

9. Er is sprake van een sterk dalende welvaart.

4.5.2 Scenario 'Bewogen' (uniform aanbod, dynamische vraag)

Scenario B is algemeen samen te vatten in de woorden: technologiestandaarden; communicatie snel & kort; MSN'en; globalisering; consolidatie; mensen hebben veel verschillende sociale contacten; 'oorlogseconomie'; veel activiteit; weinig keuze; staatsregulering; milieunormen; standaarden; zelfregulering; oligopolies; opkomst Aziatische economie en model; weinig patenten; economische groei; efficiënt; veel activiteit en verkeer; korte ontwikkelingscycli; house parties (massaal); hypes; geleide ontdekking.

4.5.2.1 Op microniveau - Bianca

Bij scenario B hoort het individu Bianca:

- Gebruiker **Bianca** (studente);
- heeft de middelen: mobiele telefoon (met achterhaalde Bluetooth-techniek (versie 1.0)), laptop, PC;
- heeft de contexten: HAN, PAN, BAN;
- gebruikt de 'klassieke' netwerken: ADSL, UMTS, GSM, Bluetooth en WiFi (in plaats van de modernere VDSL, UWB en WiMAX-netwerken die in het buitenland gemeengoed zijn);
- gebruikt onder andere de diensten: mobiel bellen, SMSen, (mobiel) e-mailen, internetten en content delen (plaatjes, muziek, spelletjes en ringtones) met haar 'buddies'.

Figuur 4.3: Bianca (studente)

Vraagkant: Bianca (19) is studente geneeskunde en fietst elke schooldag naar de universiteit. Vlak voordat ze naar college gaat, start ze haar laptop op. De laptop maakt automatisch verbinding met de aangesloten ouderwetse ADSL internetverbinding in haar HAN (haar provider biedt nog geen VDSL aan) en begint haar nieuwe e-

mailberichten te downloaden. Op het moment dat ze haar laptop dichtklapt, loskoppelt en in haar rugtas doet, pikt de laptop de UMTS internetverbinding van haar telefoon (via Bluetooth binnen haar PAN) op en gaat door met het ophalen van de e-mail. Op het moment dat ze nog niet alle e-mail heeft ontvangen kan de laptop eventueel ook nog koppelen met het netwerk van de universiteit en alsnog de laatste e-mails binnen halen. Aangekomen op de universiteit, belt ze nog even snel met haar vriendje en krijgt tijdens het gesprek een SMS-je dat het college begint. Via het draadloze netwerk van de universiteit logt ze met haar laptop automatisch aan op het WiFi netwerk (haar universiteit heeft nog steeds geen modern UWB of WiMAX-netwerk geïmplementeerd) en zo begint het college. Tussen de colleges door ziet ze haar vrienden waar ze met haar mobiele telefoon (via Bluetooth) een netwerk vormt (BAN) en haar foto's van het afgelopen weekend uitwisselt.

Aanbodkant: Hoewel Bianca redelijk veel op Ambient Networks gebaseerde diensten wil gebruiken, biedt haar universiteit deze vrijwel niet aan.

4.5.2.2 Op mesoniveau - de universiteit van Bianca

Vraagkant: De universiteit van Bianca is dusdanig ingericht dat hij lange termijn onderzoeken doet en groot en uniform is opgezet. De universiteit gaat efficiënt om met standaardprocedures en kan deze in grote massa's flexibel afhandelen. Enkele bedrijven die ook in dit scenario zouden kunnen passen zijn Philips, Aldi en Siemens [3, blz. 18]. De universiteit maakt beperkt gebruik van Ambient Networks.

Aanbodkant: Uiteraard is er een (W)LAN (Wireless Local Area Network) waar alle computers (draadloos) aan hangen. Op beperkte schaal worden hierover diensten aangeboden. Dit gaat dan vaak over een internetconnectie over het draadloze netwerk van de universiteit heen en (wanneer buiten het bereik van dit netwerk) een UMTS-verbinding. Daarnaast worden de studenten door middel van SMS-jes op de hoogte gehouden van speciale colleges en hun studieresultaten. Vanzelfsprekend is er GSM-, GPRS- en UMTS-dekking, waarvan vrijwel alle medewerkers en studenten met hun devices gebruik maken. De universiteit biedt niet actief diensten aan over deze netwerken heen, hoewel de medewerkers en studenten er klaarblijkelijk wel behoefte aan hebben. En tot slot zijn er studenten die via hun Bluetooth device een eigen BAN opzetten. Ook dit is los georganiseerd van de universiteit.

4.5.2.3 Op macroniveau - het Nederland van Bianca

Vraagkant: In het Nederland van Bianca regeert en subsidieert Brussel en is men bang voor China. Onderwijs wordt gestandaardiseerd en men leert op afstand (e-learning). Er is een sterke regulering (uit angst). Kennis homogeniseert over Europa. Autogebruik mag, mits onderworpen aan strenge regels. Openbaar vervoer wordt gestimuleerd. Men volgt qua vakantiebestemmingen de trends en vindt vermaak in de Arena met musicals en Gordon. Nederland maakt zich sterk voor een groot Europees leger en streeft naar uniforme regels [3, blz. 19].

Aanbodkant: Hoewel het Nederlandse bedrijfsleven en de Nederlanders Ambient Networks willen gebruiken (de technieken zijn aanwezig), is Europa traag met het uitgeven van uniforme regels en standaardisering zodat de uitrol van Ambient Networks word vertraagd. Het Nederland van Bianca neemt een afwachtende houding aan ten opzichte van de landen er omheen. Innovatie komt uit het buitenland en Nederland volgt.

4.5.2.4 De technologie binnen scenario 'Bewogen'

De algemene technologie binnen dit scenario is als volgt te typeren [3, blz. 20]: men werkt thuis vanwege de redelijke faciliteiten die hiervoor beschikbaar zijn (breedband Internet, via WiFi, is op straat verkrijgbaar). Men is zeer innovatief en er is een sterke groei in de nieuwe ICT-dienstverlening en -technologie. Als gevolg hiervan wordt een techniek soms te vroeg geadopteerd (met alle financiële debacles van dien). De algehele (Europese) ICT en communicatie wordt vanuit Brussel gestandaardiseerd waardoor de Nederlandse overheid zich een sterk afwachtende houding aanmeet.

4.5.2.5 De trends binnen scenario 'Bewogen'

De algemene trends binnen scenario B zijn:

Vergrijzing

1. Men werkt langer en de sociale dienstplicht is ingevoerd om ouderenzorg betaalbaar te houden.

Europa

2. Er is sprake van een federale staat: Europol, één Europees Openbaar Ministerie, één leger en productie is weer teruggehaald naar Europa.

Globalisering

3. Protectionisme als anti-reactie op producten uit Azië.

Verschuiving macht Azië

4. Koude oorlog.
5. Europa onteigent patenten.
6. Stagnering is de basis voor innovatie (behalve binnen een militaire of veiligheidscontext).

Miniaturisering

7. Massa-hype in (consumenten)elektronica (korte levensduur).
8. 'Big-Brother-staat', door spionage-devices.

Internet for Everything

9. Ultieme standaardisatie vanuit Brussel.
10. Bloei van de dienstensector en van de productie van diensten.

4.5.3 Scenario 'Complex' (divers aanbod, dynamische vraag)

Scenario C is algemeen samen te vatten in de woorden: grote diversiteit aan Customer Premises Equipment (CPE); flexibele werktijden (24 uur economie); flexibele werkplekken; maatwerk; individualistisch & interactief; veel activiteiten in vrije tijd; welvarend, met grote verschillen in welvaart; veel grote én kleine spelers in de markt; intransparant, complex dienstenaanbod; merken en merkwaarden zijn belangrijk; dienstenaanbod internationaliseert; regelgeving divers in landen/regio's; zelfverwezenlijking; alles kan, alles mag, alles gebeurt; het leven is een feest; drugs gelegaliseerd; laissez faire; anarchisme; krach om de vijf jaar; ondernemend; 'American dream'.

4.5.3.1 Op microniveau - Constantijn

Bij scenario C hoort het individu Constantijn:

- Gebruiker **Constantijn** (jonge werkende professional; 'yup');
- heeft de middelen: mobiele telefoon, laptop, PC, PDA, beeldtelefoon;
- heeft de contexten: HAN, PAN, OAN, VAN;
- gebruikt de netwerken: VDSL, GSM, WiMAX, UWB en bedrijfsnetwerk
- gebruikt onder andere de diensten: beeldbellen, mobiel bellen, SMS-en, MMS-en, (mobiel) e-mailen, internetten en data synchroniseren.

Figuur 4.4: Constantijn (yup)

Vraagkant: Constantijn (29) is een van de jongste aanwinsten van een van oorsprong Amerikaans IT-bedrijf. Op elke werkdag start Constantijn zijn op het VDSL-netwerk aangesloten thuis-PC (binnen zijn HAN) op en kijkt of hij al e-mail heeft ontvangen. Vandaag heeft hij zich verslapen. Onderweg naar de auto belt hij alvast naar zijn werk om te melden dat hij er (te laat) aankomt. In zijn auto (VAN)[23] communiceert zijn mobiele telefoon met het UWB-audiosysteem zodat hij al rijdend, zonder onderbreking, handsfree door kan bellen. Tot overmaat van ramp moet hij ook nog eens achteraan in een lange file aansluiten. Hij zet zijn laptop dan maar alvast aan die vervolgens via UWB verbinding maakt met zijn PDA en dan via het landelijke WiMAX-netwerk en uiteindelijk via Internet koppelt met het bedrijfsnetwerk, waardoor hij de laatste vergaderstukken kan downloaden op zijn laptop. Half bellend en computerend rijdt hij het bedrijfsterrein op (OAN) waarop zijn laptop direct synchroniseert met het WiMAX-netwerk (net als zijn PDA trouwens). Aangekomen op zijn werkplek, zet hij snel een beeldgesprek op met het hoofdkantoor in Amerika. Tijdens het gesprek ontvangt hij nog een MMS-je van zijn verloofde die een fotootje stuurt van het mooie Curaçao, waar zij op dat moment een internationale conferentie heeft. Zijn werkdag is begonnen en is nog lang niet afgelopen…

Aanbodkant: Constantijn is grootverbruiker van Ambient Networks diensten en zijn bedrijf biedt deze in zeer ruime mate aan.

4.5.3.2 Op mesoniveau - de organisatie van Constantijn

Vraagkant: De vlotte en snelle organisatie waar Constantijn werkt rekent haar werknemers af op de geboekte resultaten en beloont hiernaar. Het vaak ‘plat’ georganiseerde bedrijf kan zowel kleine als grote vestigingen hebben (eventueel bij de klant) en kent alleen de hoogstnoodzakelijke processen. De organisatie wordt bestuurd door een klein en efficiënt ingericht bestuursorgaan met een grote invloed. De personele bezetting kent veel wisselingen en bestaat uit veel inhuurkrachten. De diensten of producten die worden geleverd zijn veelal divers, innovatief en ‘custom-made’. Enkele

[23] …niet een bus (in het engels ‘van’), maar een klassieke Citroën C4

voorbeelden van bedrijven die in dit scenario passen zijn internetbedrijven, belhuizen, kleine consultancybedrijven en IKEA [3, blz. 10].

Aanbodkant: Het bedrijf van Constantijn kent veel diensten die gebruik maken van Ambient Networks. Zo kan hij met zijn laptop thuis, via het Internet, inloggen op het bedrijfsnetwerk, vervolgens zonder onderbrekingen overstappen op een UWB-netwerk en uiteindelijk overgaan naar het WiMAX-netwerk van zijn bedrijf. De PDA's van de medewerkers zijn binnen het bedrijf te synchroniseren met behulp van WiMAX-, of UWB-verbindingen. Daarnaast zijn bijvoorbeeld printopdrachten vanaf vele soorten devices via alle mogelijke al dan niet draadloze connecties te versturen.

4.5.3.3 Op macroniveau - het Nederland van Constantijn

Vraagkant: Het Nederland van Constantijn kent een bloeiende economie waar de overheid nieuwe initiatieven ondersteunt. Er heerst een liberale politiek met weinig regulering en wetgeving. Mensen mogen wonen waar ze willen en reizen veel (intercontinentaal). De Nederlanders zoeken veel vermaak buiten de deur (theater, outdoor sporten, vaak uit eten). Veiligheid is geen eerste prioriteit [3, blz. 11].

Aanbodkant: Het Nederland van Constantijn is zowel Europees als wereldwijd een voorloper op het gebied van Ambient Networks. De netwerken worden razendsnel uitgerold en ook kent men in Nederland veel op Ambient Networks gebaseerde diensten. De landelijke overheid stuurt aan op nieuwe initiatieven voor de uitrol van Ambient Networks (diensten). Men stuurt op innovatie en niet op regulering. Daarnaast is het Nederlandse bedrijfleven en zijn de Nederlanders actief met het ontwikkelen en gebruiken van diensten op het gebied van Ambient Networks. De EU stimuleert de ontwikkeling en adoptie van Ambient Networks en de bijbehorende dienstverlening. Veel subsidies worden toegekend aan ambitieuze en grootschalige projecten. Iedereen innoveert en wordt hierin gestimuleerd.

4.5.3.4 De technologie binnen scenario 'Complex'

De algemene technologie binnen dit scenario is als volgt te typeren [3, blz. 12]: breedband Internet is gemeengoed en er is veel mobiel verkeer met veel devices (onder andere draadloze laptops, smartphones, portable gamecomputers en PDA's), hierbij is 'roaming'[24] belangrijk. De gebruikers vertonen veel nomadisch gedrag en gebruiken een breed spectrum aan diensten, met veel content, zoals bijvoorbeeld TV op de mobiel en in de auto. Er is weinig standaardisatie voor de vele protocollen voor communicatie en er zijn dan ook veel alternatieven beschikbaar. Diensten worden 'anytime, anywhere, any country' gevraagd en aangeboden.

4.5.3.5 De trends binnen scenario 'Complex'

De algemene trends binnen scenario C zijn:

1. Miniaturisering zet door, steeds meer in één device.
2. Devices en technologie worden steeds meer bepaald door Azië (productie is ook steeds meer in Azië), standaarden worden niet meer bepaald door Europa.
3. EU voert liberaal beleid:
   - Steeds meer partijen komen op de Europese/Nederlandse markt;
   - EU standaardiseert niet meer en veilt de frequenties zonder voorgeschreven technologie.

[24] Roaming is altijd verbinding krijgen doordat de verschillende aanbieders van connectiviteit hier afspraken over hebben gemaakt.

4. Ouderen blijven actief, hebben nog genoeg te besteden en er is thuiszorg en aanvullende ondersteuning voor bejaarden om zo lang mogelijk zelfstandig te blijven wonen.
5. Vrije handel zet door met meer internationale spelers.

4.5.4 Scenario 'Degelijk' (divers aanbod, statische vraag)

Scenario D is algemeen samen te vatten in de woorden: vaste winkelformules (franchise; Primafoon); Luxe: het komt naar je toe; consumenteneconomie; Onderwijs: op maat gesneden aanbod op vaste plekken; Romeinse rijk ten tijde van Nero en Caligula; Diversiteit komt van aanbod uit China; Deconsolidatie; versnippering van bedrijven en instellingen; Nederland; Buyersmarket; Antiglobalisering / Greenpeace / Alto; Cocooning; Blowen / drugsgebruik; Onthaast; Groen-links.

4.5.4.1 Op microniveau - Deborah

Bij scenario D hoort het individu Deborah:

- Gebruiker **Deborah** (secretaresse);
- heeft de middelen: mobiele telefoon, vaste telefoon, PC;
- heeft de contexten: HAN, OAN, PAN;
- gebruikt de netwerken: ADSL, bedrijfsnetwerk, vaste telefonienetwerk, GSM;
- gebruikt de diensten: mobiel bellen, 'vast' bellen, e-mailen en internetten.

Figuur 4.5: Deborah (secretaresse)

Vraagkant: Deborah (59) is secretaresse bij een groot Nederlands bedrijf. Deborah werkt drie dagen per week en reist met de bus naar haar werk. Terwijl ze in de bus zit belt ze nog snel even met haar kleindochter die haar vraagt of oma ook *MSN+ Virtual Chat2016™* heeft. Deborah snapt niet wat MSN is, hoewel ze wel Internet thuis heeft. (Haar breedbandverbinding is nog gebaseerd op ADSL-techniek; ze ziet nog geen aanleiding om over te stappen op VDSL.) Aangekomen bij haar werk, logt ze in en zoekt op Internet naar een hotel voor haar baas. Ze belt het hotel en reserveert een kamer. Boeken via Internet durft ze niet aan. Vervolgens belt ze haar baas op dat er een kamer is geboekt. Terwijl ze haar baas aan de lijn heeft, vraagt deze haar of ze ook een PDA met WiMAX en UWB wil (omdat dat zo makkelijk is). Deborah weet niet precies wat een PDA is en zegt dat ze haar zelf goed kan redden met een vaste telefoon en haar

mobiele telefoon (als mensen maar niet te vaak bellen). Na een lange werkdag komt ze moe thuis en belt nog even met haar zus. De dag is voorbij.

Aanbodkant: Hoewel Deborah niet veel op Ambient Networks gebaseerde diensten gebruikt, biedt haar omgeving die wel aan. Ze hoeft ze echter niet.

4.5.4.2 Op mesoniveau - de werkgever van Deborah

Vraagkant: Deborahs werkgever produceert veel in lage lonen landen. Het bedrijf profileert zich als een 'feel good' organisatie en kent relatief veel deeltijdbanen. Kwaliteit is belangrijk voor de organisatie. Het bedrijf is hiërarchisch ingericht en medewerkers blijven lang werken bij dit bedrijf. Enkele voorbeeldbedrijven die voldoen aan deze beschrijving voor dit scenario zijn Nike, AH, Marktplaats.nl en KPN [3, blz. 34].

Aanbodkant: Het bedrijf kent niet overdreven veel diensten die gebruik maken van Ambient Networks. Hoewel de mogelijkheden er wel zijn, worden deze niet altijd benut. Zo is de technologie aanwezig om het hele bedrijfsnetwerk draadloos te maken, maar dit staat al vijf jaar op de agenda en is nog steeds niet geïmplementeerd. Ook zijn er diensten mogelijk waarbij mobiele internettoegang over meerdere netwerken heen mogelijk wordt gemaakt. De organisatie heeft er echter geen behoefte aan.

4.5.4.3 Op macroniveau - het Nederland van Deborah

Vraagkant: De economie van het Nederland van Deborah is op zijn retour. Men beschermt wat men heeft. Ook veel politieke partijen zijn op hun retour. Er zijn maatschappelijke spanningen (er wordt over 'wij en zij' gesproken). Mensen gaan veel buiten de stad wonen waardoor er veel woon-werkverkeer is. Nederlanders kennen een lage arbeidparticipatie. Men leert wat leuk is, maar dat hoeft niet noodzakelijk goed te zijn voor de carrière [3, blz. 35].

Aanbodkant: De Nederlandse markt en overheid stimuleren initiatieven op het gebied van Ambient Networks (diensten). Ook Europa stimuleert de ontwikkeling en uitrol van Ambient Networks en diensten. Europa kent veel subsidies toe aan grootschalige projecten. Echter de Nederlanders en het bedrijfsleven willen het niet.

4.5.4.4 De technologie binnen scenario 'Degelijk'

De algemene technologie binnen dit scenario is als volgt te typeren [3, blz. 36]: er is een groot aanbod van hoogwaardige telecommunicatiediensten (denk aan HDTV); huishoud- en persoonlijke elektronica is steeds meer geïntegreerd. De gebruikers echter zijn gefocusseerd op bestaande diensten (eventueel op nieuwe technologie).

4.5.4.5 De trends binnen scenario 'Degelijk'

De algemene trends binnen scenario D zijn:

Vergrijzing

1. Er is een sterke druk op de zorgsector; tweedeling;
2. Risico voor de Nederlandse regelgeving.

Europa

3. Protectionisme op Europese schaal.

Verschuiving economische macht naar Azië

4. Europa wordt een dienstverlenende economie.

Miniaturisering

5. Voor alle behoeften geldt dat deze 'perfect' (ergonomisch, goedkoop) moeten worden ingevuld, apparatuur is hierom vaak modulair opgebouwd.

Internet for Everything

6. Geen verschil tussen tv, audio en communicatie (‘triple play’)[25].

4.6 Conclusie

De vraag naar en het aanbod van Ambient Networks (AN) en de bijbehorende diensten zijn per scenario samengevat in de onderstaande tabel:

Scenario	**Vraag naar AN**	**Aanbod van AN**
Afwachtend	Hier is vrijwel geen vraag naar AN diensten. Alleen wanneer het echt niet anders kan stapt de vrager over op ‘nieuwe’ techniek.	Ook hier is men afwachtend. De dienstaanbieders wachten af wat Europa doet. • vaste bedrijfsnetwerken • bekende draadloze en bedrade communicatie-netwerken (GSM, ADSL, …) • hier-en-daar ‘nieuwe’ technologiën (VoIP)
Bewogen	De vraagkant is te typeren als gretig. Men wil AN diensten afnemen, maar word geremd door de aanbodkant.	De aanbieders van diensten innoveren vrijwel niet en hebben een afwachtende houden. Zij zijn de rem op de ontwikkeling van Ambient Networks. • vaste bedrijfsnetwerken • bekende draadloze en bedrade communicatie-netwerken (GSM, ADSL, …) • hier-en-daar nieuwe technologiën (VoIP)
Complex	De vrager wil en kan alles. AN worden maximaal gebruikt.	AN diensten worden in zeer ruime mate aangeboden. • Alle nieuwe draadloze en bedrade netwerken door elkaar heen (VDSL, WiMAX, UWB, …)
Degelijk	Ook hier is vrijwel geen vraag naar AN diensten.	Hier worden veel AN diensten aangeboden. • Alle nieuwe draadloze en bedrade netwerken door elkaar heen (VDSL, WiMAX, UWB, …)

Tabel 1: Samenvatting van de scenario’s.

[25] Met ‘triple play’ wordt bedoeld dat een aanbieder zowel digitale (IP)televisie, VoIP als Internet aanbiedt.

5 Security aspecten en maatregelen

In dit hoofdstuk worden de security aspecten van Ambient Networks beschreven. Dat zijn (1) de specifieke technische kwetsbaarheden voor Ambient Networks en de dreigingen die van deze kwetsbaarheden uitgaan, daarnaast de algemene (niet-technische) kwetsbaarheden en dreigingen en tot slot (3) enkele omgevingsaspecten die relevant kunnen zijn voor security binnen Ambient Networks. Daarnaast worden nog de beveiligingsmaatregelen die tegen deze security aspecten genomen kunnen worden weergegeven. Dit is nog even los van de vraag- en aanbodkant in de markt en de hiervoor genoemde vier scenario's. Dit hoofdstuk gaat over de daadwerkelijke security aspecten en maatregelen en dient als input voor de security visie in hoofdstuk zes.

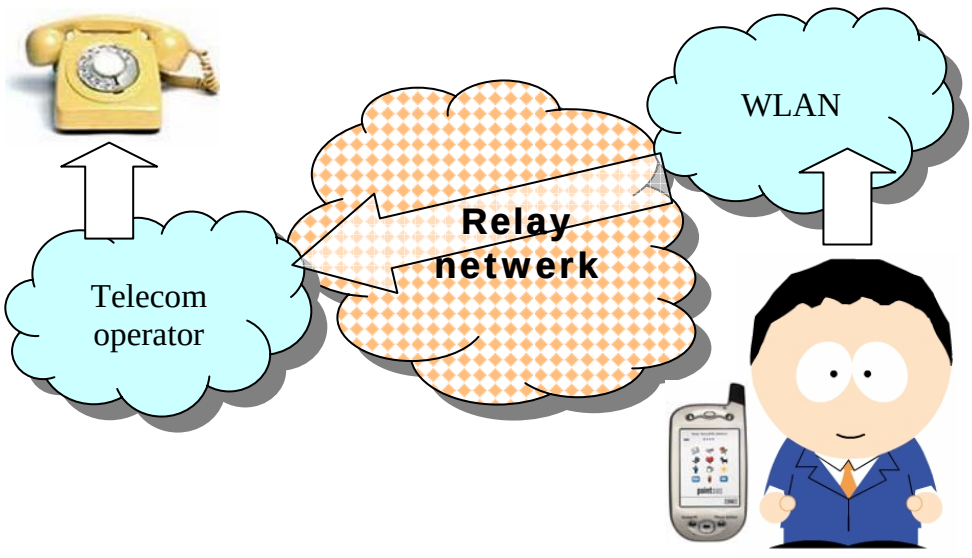
5.1 De security aspecten

Zoals gezegd eerst de security aspecten, verdeeld over drie subparagrafen:

- Technische kwetsbaarheden en dreigingen
- Algemene (niet-technische) kwetsbaarheden en dreigingen
- Omgevingsaspecten

5.1.1 Technische kwetsbaarheden en dreigingen

Deze paragraaf bevat de technische kwetsbaarheden en dreigingen die *specifiek voor Ambient Networks* gelden, waarbij naar de typische kenmerken zoals de snelle, dynamische en kortstondige communicatie van Ambient Networks wordt gekeken. Er wordt hier niet gekeken naar de algemene dreigingen die uitgaan van de losse technieken. Het gaat dus specifiek om die kwesties die juist kenmerkend zijn voor Ambient Networks en hierdoor bepalend voor de (technische) security aspecten. Het gebruik van relay netwerken is een dergelijke kwestie binnen Ambient Networks.



Figuur 5.1: Het gebruik van relay netwerken in Ambient Networks

In Figuur 5.1 wordt het principe van relay netwerken geïllustreerd met een voorbeeld: Constantijn wil een telefonische verbinding opzetten via het lokale WLAN. Omdat het WLAN geen directe verbinding heeft met het netwerk van de telecom operator, wordt

ad-hoc het WLAN gekoppeld met een nabijgelegen netwerk wat wel is verbonden met de telecom operator. Via de telecom operator kan uiteindelijk de gewenste telefonische verbinding worden opgezet. Constantijn is als gebruiker aangemeld bij het WLAN netwerk en is bekend bij de telecom operator, maar het tussenliggende netwerk, het zogenaamde relay netwerk, heeft niet op voorhand een relatie met Constantijn en ook niet met het lokale WLAN. In deze paragraaf zal o.a. worden ingegaan op de technische security problemen die het gebruik van relay netwerken met zich meebrengt.

De hieronder beschreven technische aspecten komen uit het project “Ambient Network Security Architecture” [4, blz. 16-17]. Bij de eerste zeven aspecten, die zijn gerangschikt naar afnemende relevantie voor Ambient Networks, zijn enkele dreigingen te benoemen. Echter, er zijn ook aspecten waar geen dreigingen vanuit gaan, maar waar security wel een rol speelt. Deze worden aan het eind van deze paragraaf vermeld.

1. *Toegang tot netwerken*: er zijn diverse netwerken waar een gebruiker toegang tot zou kunnen krijgen. In Ambient Networks moet de keuze voor bepaalde netwerken flexibel zijn. In sommige gevallen moet het mogelijk zijn om toegang te krijgen zonder inschrijving vooraf. Dit vraagt in de toekomst om een andere aanpak van toegangscontrole. Een ander scenario is dat toegang tot een netwerk alleen mogelijk is via een aantal tussenliggende (ad-hoc) netwerken. Op een of andere manier moeten de tussenliggende ‘relay’ netwerken voor deze diensten worden gecompenseerd, zelfs als er geen a-priori relatie met deze gebruiker is. In het voorbeeld van Figuur 5.1 draagt het relay netwerk bij aan de telefonische verbinding van Constantijn, waar de eigenaar van het relay netwerk redelijkerwijs een financiële compensatie voor mag verwachten. Constantijn is als gebruiker echter niet bekend bij dit relay netwerk.
   Dreiging:
   - Wanneer de toegang tot de netwerken niet goed is geregeld (bijvoorbeeld als gevolg van onduidelijk beleid), of wanneer er zwakheden zijn die uitgebuit kunnen worden (als gevolg van een bug in de hardware), kunnen kwaadwillenden onrechtmatig toegang krijgen tot de netwerken en persoonlijke informatie.
2. *Mobiliteitsmechanismen*: om te zorgen dat de communicatie kan voortgaan, zelfs bij veranderingen in de IP verbinding, zijn mobiliteitsmechanismen ontwikkeld om bijvoorbeeld verschillende toegangspunten tegelijkertijd te kunnen gebruiken. Zo zal er bijvoorbeeld in Figuur 5.1 een mobiliteitsmechanisme moeten zijn dat ad-hoc bepaalt welk relay netwerk het beste geschikt is voor de telefonische verbinding van Constantijn.
   Dreiging:
   - Dergelijke mechanismen zijn echter gevoelig voor misbruik. Een aanvaller zou een verzoek kunnen doen voor verplaatsing van andermans verbindingen richting hem, of zou andermans verbindingen kunnen ‘bombarderen’ met intensieve verkeersstromen. Hier zijn wel maatregelen tegen te nemen, maar die gaan vaak ten koste van een vertraging in de verbinding.
3. *Netwerkkoppelingen*: traditioneel wordt de toegang tot netwerken per device geregeld, maar in Ambient Networks zal eerder getracht worden om hele netwerken (tijdelijk) te koppelen. Bijvoorbeeld een Personal Area Network (PAN) wat wordt gekoppeld aan een Vehicular Area Network (VAN). Hierbij worden dan rechten toegekend op basis van de verschillende rollen van de deelnemers, ook voor de diensten die op die netwerken worden aangeboden. Een onderdeel hiervan zijn de *roaming* procedures[24]. In het voorbeeld van Figuur 5.1 zou de beheerder van het WLAN kunnen overwegen om niet langer op een ad-hoc manier voor elke verbinding een relay netwerk te kiezen, maar om op netwerkniveau op voorhand koppelingen te maken met een beperkt aantal zorgvuldig gekozen (relay-)netwerken.

Dreiging:

- Een fraudeur zou eventuele zwakheden in de netwerkkoppelingen (bijvoorbeeld met betrekking tot de authenticatie- en autorisatieprocedures, maar ook de roaming procedures) kunnen uitbuiten om geld te verdienen door de tarieven zo toe te passen dat hij er financieel voordeel bij heeft.

4. *De IP verbinding*: bovenop de (flexibele) fysieke verbinding moet een stabiele IP verbinding draaien over de juiste routers. Er mag geen vertraging of security probleem ontstaan bij een transfer van de fysieke verbinding. In de huidige situatie wordt een IP verbinding pas opgezet nadat toegang tot het netwerk is verleend, maar in Ambient Networks zou dat gelijktijdig moeten gebeuren. Verder kent het IP protocol verschillende mechanismen (zoals Network Address Translation) voor omgang met verschillende administratieve domeinen. De hoeveelheid aan IP adressen maakt IPv6 geschikt voor Ambient Networks.
   Dreiging:
   - De verschillende aanpakken binnen de domeinen kan echter end-to-end security in de weg staan. Als voorbeeld is de beveiliging van de telefonische verbinding van Constantijn in figuur 5.1 sterk afhankelijk van de security mechanismen in de tussenliggende netwerken en hoe die op elkaar zijn afgestemd. Daarnaast is de IP-verbinding gevoelig voor aanvallen via Internet waaronder denial-of-service aanvallen op devices en netwerken.
5. *De fysieke verbinding*: hierbij gaat het om aspecten als het opzetten van de draadloze verbinding tussen devices, het in de gaten houden van de zendkracht en andere kwaliteitsaspecten (QoS), de transfer van de verbinding naar andere domeinen, bescherming van de pakketten, et cetera. Bij Ambient Networks zal er vaak met behulp van vaste of draadloze technologieën naar andere domeinen getransfereerd dienen te worden waar de beveiliging van de verbinding geen last van mag ondervinden. In het voorbeeld in figuur 5.1 gaat het bijvoorbeeld om de koppelingen tussen het WLAN, het tussenliggende relay netwerk, en het netwerk van de telecom operator.
   Dreiging:
   - Kwaadwillenden kunnen inbreken op de draad(loze)verbinding en zo de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatie aantasten.
6. *Beheer en autorisatie van middelen*: de verschillende middelen (zie 2.1) in een Ambient Network moeten worden beheerd. Elk middel heeft zijn eigen autorisaties: rechten om toegang te krijgen tot netwerken, diensten, systemen, bestanden, et cetera.
   Dreiging:
   - Wanneer de verschillende middelen niet goed worden beheerd is de kans op kwetsbaarheden groter omdat hardware niet gepatchd en software niet geüpdatet wordt.
7. *Compatibiliteit*: een Ambient Network moet kunnen communiceren met (oudere) reeds bestaande netwerken. Dat betekent o.a. dat verschillende mobiliteitsmechanismen moeten worden ondersteund.
   Dreiging:
   - Wanneer oude en nieuwe systemen puur functioneel compatibel zijn (en er is verder in het ontwerp geen rekening gehouden met security), is de kans aanwezig dat kwaadwillenden zwakheden vinden in de implementatie van de systemen en zo in kunnen breken waardoor de informatie kwetsbaar wordt.

Naast de technische security aspecten, waar dreigingen vanuit gaan, zijn er ook technische aspecten waar geen dreigingen vanuit gaan, maar waar security wel een rol kan spelen:

- *Gebruik van context informatie*: wanneer de knooppunten van een Ambient Network zich bewust worden van de soorten diensten en devices die in hun omgeving beschikbaar zijn, kan die informatie nuttig gebruikt worden voor bijvoorbeeld security. Bij overschakeling van een bedrijfsnetwerk naar een publiek netwerk zou de verbinding bijvoorbeeld automatisch vercijferd kunnen worden.
- *Communicatie binnen groepen*: de verschillende groepen die binnen een Ambient Nework willen communiceren, hebben elk hun eigen groepssleutel om de communicatie te vercijferen. Dit vraagt om nieuwe cryptografische mechanismen. Ook broadcast en multi-cast functies (uitzendingen) vallen hieronder.

5.1.2 Algemene kwetsbaarheden en dreigingen

In dit deel wordt ingegaan op de kwetsbaarheden en dreigingen van Ambient Networks die minder technisch van aard zijn. De onderwerpen zijn afkomstig van het Europese project “Safeguards in a World of Ambient Intelligence” (SWAMI)[26] [5] [6].

In [5, blz. 8] worden een aantal sleutelgebieden genoemd binnen de wereld van Ambient Intelligence, die ook betrekking hebben op de Ambient Networks. Binnen elk van deze sleutelgebieden zijn in [6] de belangrijkste dreigingen geïnventariseerd en geprioriteerd op volgorde van afnemende relevantie voor Ambient Networks:

8. *Vertrouwen*: doordat contacten met personen en systemen in Ambient Networks vaak ‘vluchtig’ van aard zijn, is er nauwelijks gelegenheid voor het opbouwen van een vertrouwensrelatie. Vanuit security oogpunt is het wel belangrijk dat componenten kunnen worden vertrouwd, dus zal er naar andersoortige oplossingen gezocht moeten worden. Zo zal bijvoorbeeld in figuur 5.1 het WLAN zorgvuldig een geschikt relay netwerk moeten kiezen om een betrouwbare telefonische verbinding voor Constantijn op te kunnen zetten. Doordat er op voorhand geen relatie is tussen het WLAN en het relay netwerk is er behoefte aan een alternatief wederzijds vertrouwensmechanisme.
   Dreiging:
   - Doordat er bij Ambient Networks veel communicatie en processen ‘op de achtergrond’ lopen, is het moeilijk voor een gebruiker om zicht te krijgen op wat er precies gebeurt. Hierdoor is hoe omgegaan wordt met persoonlijke informatie onduidelijk en dat gaat ten koste van het vertrouwen in de systemen. Dit heeft ook als gevolg dat de vertrouwelijkheid van de informatie niet altijd te garanderen is omdat gebruikers hun informatie wellicht wel toevertrouwen aan een onvertrouwd systeem.
   - Binnen de Ambient Networks visie staat de gebruiker centraal. Dat betekent dat veelvuldig gebruik zal worden gemaakt van persoonlijke profielen op basis waarvan diensten kunnen worden afgenomen en toegang tot systemen wordt geregeld. Dat maakt het persoonlijke profiel erg gevoelig en kwetsbaar. Want als een profiel onvolledig is (door een moedwillige aanval hierop) of lijkt (de gebruiker kan hier om privacy redenen voor gekozen hebben) of verkeerd wordt geïnterpreteerd, kan onterecht toegang tot diensten of systemen worden geweigerd. Dus door de verhoogde kwetsbaarheid van het persoonlijke profiel kan het vertrouwen van de gebruiker in de systemen worden aangetast.

[26] http://swami.jrc.es

9. *Technische complexiteit*: Door de hoge mate van afhankelijkheid van systemen, maar vooral de toegenomen complexiteit van computersystemen ("*…security en complexiteit gaan niet samen"*[27]) is een hoog kennisniveau nodig voor de beveiliging. Bij veel gebruikers ontbreekt deze kennis, daarbij is er ook een gebrek aan gebruikersvriendelijke security mechanismen.
   Dreiging:
   - Door de complexiteit van Ambient Networks is de kans op opzettelijk misbruik van diensten, systemen of gegevens groot, waarbij de beschikbaarheid, vertrouwelijkheid en integriteit van informatie in het gedrang komt. Het doel kan financieel gewin zijn, maar ook frustratie van systemen of het spioneren van personen.
   - De security kan ook zonder opzet (als gevolg van de complexiteit) in gedrang komen. Bijvoorbeeld door een fout in het ontwerp van systemen, gebrek aan gebruikersvriendelijkheid, compatibiliteit van systemen, of gebrek aan security kennis.
10. *Privacy*: door de veelheid aan persoonlijke gegevens en mogelijkheden om personen te volgen, is privacy een belangrijk aandachtspunt binnen Ambient Networks.
    Dreiging:
    - Stiekem verzamelde persoonsgegevens kunnen voor andere doeleinden gebruikt worden dan aanvankelijk bedoeld.
    - Gebruikers zijn te weinig bewust van hun privacy rechten (ze zijn weinig 'aware') en daardoor zijn ze geneigd om hun informatie open en bloot aan te bieden (omdat ze niet beter weten) waardoor hun informatie wellicht kwetsbaar is voor bijvoorbeeld aanvallen (op de privacy).
11. *Identiteitsmanagement*: in Ambient Networks kent elke persoon of elk device meerdere identiteiten afhankelijk van de context (zie 2.2) waarop de identiteit betrekking heeft. Aangezien veel diensten over meerdere domeinen gaan is er een behoefte om de verschillende identiteiten aan elkaar te kunnen relateren zodanig dat het beheersbaar blijft en de gebruiker controle houdt. Daarnaast verhoogt de veelheid aan identiteiten tevens de kans op misbruik ervan. In het voorbeeld van figuur 5.1 betekent dit: Constantijn is als gebruiker bekend bij het WLAN en heeft daar een bepaalde identifier (bijvoorbeeld superyup@local.nl). Tevens is hij geregistreerd als klant bij de telecom operator (bijvoorbeeld als constantijn@company.com). Voor het opzetten van de telefonische verbinding is het noodzakelijk dat de telecom operator Constantijn daadwerkelijk herkend als constantijn@company.com, een identifier die op voorhand binnen de WLAN context geen betekenis heeft.
    Dreiging:
    - Het 'stelen' van identiteiten en daarmee de mogelijkheid voor kwaadwillenden om zich voor te doen als andere personen.
    - Het ongewenst relateren van verschillende identiteiten van eenzelfde persoon om daarmee een privacy gevoelig profiel op te bouwen.
12. *De digitale kloof*: de kloof in de huidige maatschappij tussen personen die mee kunnen en willen gaan met nieuwe ontwikkelingen in de ICT en personen die dat niet kunnen of willen, zal door de komst van Ambient Networks alleen maar groter worden.
    Dreiging:

[27] http://www.cs.ru.nl/B.Jacobs/PAPERS/ag-security04.txt, september 2004 (Bart Jacobs, hoogleraar Beveiliging en Correctheid van Programmatuur, Nijmeegs Instituut voor Informatica en Informatiekunde (NIII), Radboud Universiteit)

- Door deze digitale kloof, die versterkt wordt door de komst van Ambient Networks, zal de persoonlijke informatie van de gebruikers die er niets van willen of kunnen weten (en toch afhankelijk zijn van de techniek) potentieel kwetsbaar zijn.
- Het persoonlijke profiel zal een prominentere plaats innemen in het gebruik van digitale diensten. Het niet kunnen of willen aanpassen van een persoonlijk profiel kan leiden tot een verdere uitsluiting van de digitale wereld en maakt de persoonlijke informatie van gebruikers kwetsbaar.

5.1.3 Omgevingsaspecten

Er zijn ook een aantal omgevingsaspecten voor Ambient Networks te noemen [9] die van belang zijn voor het security beleid. De meeste zijn overgenomen uit “Herijking ICT veiligheidsbeleid” [9]:

13. *Een toenemende afhankelijkheid van ICT*: voor het besturen en beheren van maatschappelijke kernvoorzieningen maken zowel publieke als private actoren steeds meer gebruik van ICT. De kwetsbaarheid hiervan heeft gevolgen voor het functioneren van de samenleving en het dagelijkse leven.
    Dreiging:
    - Omdat maatschappelijke kernvoorzieningen meer-en-meer afhankelijk lijken te worden van ICT (en ICT niet altijd de veiligste methode is gebleken, in vergelijking met ‘ouderwetse’ papieren, formulieren en kaartenbakken) is de informatie van de gebruikers potentieel meer kwetsbaar.
14. *Een gefragmenteerde omgeving*: de dynamische omgeving wordt meer gefragmenteerd door de veelheid aan partijen, de onduidelijkheid tussen oorzaak en gevolg en de internationale dimensie.
    Dreigingen:
    - Onduidelijkheid als gevolg van een gefragmenteerde omgeving kan leiden tot onoplettendheid, desinteresse of frustratie bij gebruikers en beheerders van netwerken en devices. Dit kan resulteren in een kwetsbare omgeving waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie in gevaar komt.
    - Door gebrek aan transparantie in de markt en is het lastiger om stabiele Service Level Agreements af te spreken tussen de verschillende partijen. Dit verhoogt de technische kwetsbaarheid van de samenleving.
15. *Professionalisering van cybercrime*: ICT wordt voor criminelen een steeds interessanter werkterrein.
    Dreiging:
    - Cybercrime gaat met zijn tijd mee en professionaliseert. Daarbij komt ook dat er meer ‘te halen’ is in de digitale ICT-omgeving. Naar aanleiding hiervan is ook hier de informatie van de gebruikers kwetsbaar.
16. *Gebrek aan beveiligingsbewustzijn bij gebruikers*: Het gebruik van Ambient Networks diensten en devices door eindgebruikers kan wellicht slordig zijn. Zo kan men, vanuit een gebrek aan beveiligingsbewustzijn, zomaar de connectie verbreken of juist zomaar ergens connectie mee maken.
    Dreiging:
    - Dit gebrek aan beveiligingsbewustzijn kan ook leiden tot onoplettendheid, desinteresse of frustratie bij gebruikers van netwerken en devices. Dit kan resulteren in een kwetsbare omgeving waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie in gevaar komt.

5.2 Maatregelen tegen de security aspecten

Naar aanleiding van de vorige drie paragrafen zijn vanuit de literatuur [2, 4, 5, 6, 9] en TNO's eigen kennis en ervaring een aantal beveiligingsmaatregelen te definiëren in antwoord op de security aspecten. De nummering van deze maatregelen refereert naar de kwetsbaarheden, dreigingen en omgevingsaspecten uit de voorgaande drie paragrafen waarvoor deze maatregelen bedoeld zijn.

Tot slot volgen nog wat aanvullende maatregelen. Deze hebben een technisch, sociaal-economisch en juridisch karakter. En aan het eind wordt nog ingegaan op maatregelen die specifiek voor de gebruiker gelden. Deze set aanvullende maatregelen nummert weer opnieuw.

5.2.1 Maatregelen bij de technische kwetsbaarheden en dreigingen

Allereerst de specifieke maatregelen die specifiek gelden voor de in voorgaande drie paragrafen genoemde kwetsbaarheden en dreigingen:

1. *Toegang tot netwerken*: de operators van de netwerken dienen een continu beveiligingsproces (inclusief risicoanalyses) op orde te hebben waarbij gestuurd wordt op een planmatige beheersing van de (potentiële) risico's ten aanzien van de toegang tot de netwerken. Dit proces is vooral een bestuurlijk proces (bijvoorbeeld gebaseerd op een managementsysteem voor informatiebeveiliging, zoals voorgesteld in de ISO27001[28]), maar wordt concreet ingevuld met maatregelen (uit bijvoorbeeld de ISO17799[29]). Merk op dat deze twee ISO-normen breder zijn gedefinieerd dan alleen de toegang tot netwerken.
2. *Mobiliteitsmechanismen*: de netwerkoperators en service providers dienen de mobiliteitsmechanismen adequaat te beveiligen om fraude door buitenstaanders te voorkomen. Zij zullen hiervoor per communicatietechniek de verschillende fraudescenario's moeten inventariseren en de juiste maatregelen treffen. Uiteraard dient hier ene risicoanalyse aan voor te gaan.
3. *Netwerkkoppelingen*: naast de beveiliging tegen de ongeautoriseerde toegang tot de netwerken (maatregel 1) dienen met name de netwerk operators en fabrikanten tot in detail gespecificeerde technische protocollen voor specifieke koppelingen tussen de verschillende netwerktechnieken op te stellen en te onderhouden. Uiteraard zal dit internationaal moeten worden aangepakt om een wereldwijde werking van Ambient Networks te garanderen.
4. *De IP-verbinding:* er dient door de netwerkoperators, service providers en fabrikanten kennis te worden opgedaan hoe met de problematiek rondom de IP-verbinding moet worden omgegaan. IPv6 is hierbij leidend.
5. *De fysieke verbinding*: in de daadwerkelijke technische protocollen binnen Ambient Networks, en hoe deze zijn geïmplementeerd op de apparaten (middelen van de gebruiker en de verschillende componenten in het netwerk), dient security adequaat te zijn meegenomen in de specificaties. Daarnaast dienen fabrikanten zich aan de specificaties voor deze protocollen te houden en dienen ze zorg te dragen voor handleidingen voor de juiste installatie en gebruik van hun producten.
6. *Beheer en autorisatie van middelen*: al het beheer en de autorisaties van de veelheid aan devices binnen de netwerken moet door de netwerk operators en service providers beheerd worden: nieuwe devices die verschijnen, oude devices die

[28] Voorheen was dit altijd de BS7799-2.

[29] Voorheen was dit altijd de BS7799-1. De ISO17799 zal in de nabije toekomst ISO27001 gaan heten. (In de volksmond worden deze twee normen samen ook wel de CIB (Code voor Informatiebeveiliging) genoemd.)

verdwijnen of van eigenaar wisselen, et cetera. Voor elk type device (middel) dient een eigenaar te zijn en dient een rol te zijn gedefinieerd waarbij ingegaan wordt op wat een rol mag met zijn device.

7. *Compatibiliteit*: met name fabrikanten en netwerk operators dienen rekening te houden met oudere (reeds bestaande) netwerken en devices. Zo moet bijvoorbeeld het authenticatie framework (beheerd door de netwerk operators) oudere 'credentials' (zoals SIM kaarten) ondersteunen.

5.2.2 Maatregelen bij de algemene kwetsbaarheden en dreigingen

8. *Vertrouwen*: om de vertrouwensrelatie tussen de verschillende componenten (middelen van de gebruiker, apparaten in het netwerk) te verbeteren kunnen door de netwerkoperators en service providers elektronische certificaten worden toegepast, waarmee wordt bewezen dat de netwerkoperators en service providers (en daarmee hun systemen) vertrouwd kunnen worden. Hiermee zijn onder andere de profielen (persoonlijke data) van de gebruikers beter te beveiligen.
9. *Technische complexiteit*: deze complexiteit binnen de technische systemen kan enigszins worden voorkomen door netwerk operators en service providers het beheer van de systemen decentraal te laten inrichten.
10. *Privacy*: de overheid dient de privacybescherming van de gebruikers (juist binnen de Ambient Networks context) in de juiste bewoordingen vast te leggen in wet- en regelgeving. Daarnaast dienen de netwerkoperators en service providers met deugdelijke authenticatie- en autorisatie processen de privacy van de gebruikers te waarborgen. Daarnaast dienen gebruikers zich er ook van bewust te zijn dat ze op hun privé-gegevens moeten passen.
11. *Identiteitsmanagement*: om de identiteitsmanagement problematiek op te lossen dienen de netwerkoperators en service providers deugdelijke identiteitsmanagement systemen te implementeren (al of niet vanuit wet- en regelgeving van de overheid). (Globaal is dit dezelfde maatregel als hierboven, hoewel het verder gaat dan alleen maar de implementatie van authenticatie- en autorisatie processen.)
12. *De digitale kloof*: de overheid zal de zwakke groep die zich niet wil of kan aanpassen aan de moderne technieken (en hierdoor kwetsbaar is) moeten beschermen. De service providers zullen in sommige toekomstscenario's namelijk minder geneigd zijn om dit te doen.

5.2.3 Maatregelen bij de omgevingsaspecten

13. *Een toenemende afhankelijkheid van ICT*: vanwege de toenemende afhankelijkheid van ICT bij de maatschappelijke kernvoorzieningen dienen netwerk operators, service providers en fabrikanten in te spelen op de toenemende behoefte aan 'governance'[30]. Hiermee dienen zij controle over de beveiligingsrisico's binnen hun IT-processen aantoonbaar te maken. Daarnaast dienen deze partijen differentiatie in de risico's aan te brengen bij het invullen van governance.
14. *Een gefragmenteerde omgeving*: verantwoordelijkheden zullen helder moeten worden gemaakt en moeten worden opgepakt door de netwerkoperators en service providers. Verder kan de overheid aansturen op internationale samenwerking.
15. *Professionalisering van cybercrime*: de overheid zal meer zichtbare aandacht voor preventie, opsporing en vervolging van cybercrime moeten hebben. Daarnaast zullen netwerk operators, service providers, fabrikanten en gebruikers zich er meer bewust van moeten zijn en worden.

[30] Governance is niet meer en niet minder dan de besturing van IT door de hoogste geleding van de organisatie, gewoonlijk de Raad van Bestuur.

16. *Gebrek aan beveiligingsbewustzijn bij gebruikers*: de gebruiker moet zich bewust worden van de beveiligingsrisico's die hij of zij loopt. In eerste instantie hebben de overheid en de service providers hierin een voorlichtende taak.

5.2.4 Aanvullende maatregelen

Tot slot worden in [6] ook een aantal, redelijk voor de hand liggende, algemene maatregelen genoemd waarmee de genoemde dreigingen kunnen worden beperkt. Deze maatregelen gelden op technisch, sociaal-economisch als juridisch vlak. Daarnaast zijn er nog maatregelen specifiek voor de gebruiker.

5.2.4.1 Algemene technische maatregelen

1. *Opslag van persoonsgegevens minimaliseren*: De netwerk operators en service providers dienen de verzameling, transmissie en opslag van persoonsgegevens tot alleen de essentiële gegevens te minimaliseren die voor dat doel benodigd zijn.
2. *Veilige autorisatie*: De netwerk operators en service providers dienen zorg te dragen voor een veilige inrichting van de autorisatie van personen en de installatie van de laatste antivirus software.
3. *Toepassing van pseudoniemen*: De netwerk operators dienen op netwerkniveau gebruik te maken van privacy beschermende oplossingen (bijvoorbeeld op basis van pseudoniemen). Service providers dienen dit op dienstniveau te doen.

5.2.4.2 Algemene sociaal-economische maatregelen

4. *Stimuleren van open standaarden*: De overheid, netwerk operators en service providers dienen het gebruik van open standaarden te stimuleren. Het gebruik van open standaarden stimuleert namelijk de transparantie in de markt en de marktwerking. Bovendien is vanuit een beveiligingstechnisch perspectief het gebruik van open standaarden aan te bevelen omdat deze standaarden door vele verschillende experts al kritisch zijn bekeken waardoor de kans op mogelijke beveiligingsrisico's wordt verkleind.
5. *Keurmerken t.b.v. vertrouwen*: De overheid, de netwerk operators en service providers zouden zorg kunnen dragen voor keurmerken en reputatie systemen om het vertrouwen te vergroten.
6. *Kennis op peil houden*: De netwerk operators, service providers en fabrikanten zijn verantwoordelijk voor het op peil houden van de kennis van nieuwe technologieën door middel van scholing en cursussen.

5.2.4.3 Algemene juridische maatregelen

7. *Wet- en regelgeving toekomstbestendig maken*: De overheid dient er zorg voor te dragen dat wetgeving zoveel mogelijk toekomstbestendig is en toepasbaar blijft op nieuwe technologieën.
8. *Digitaal territorium*: Service providers dienen het concept van het digitale territorium toe te passen waarbinnen een gebruiker zich 'thuis' zou moeten kunnen voelen. Met het digitale territorium wordt het privé-terrein van een gebruiker in de digitale wereld bedoeld. Binnen dit territorium moet streng voor de privacy van de gebruiker worden gewaakt.
9. *Controle over persoonlijke informatie voor de gebruiker*: De netwerk operators en service providers dienen de systemen zo in te richten dat de gebruiker de controle heeft over al zijn persoonlijke informatie.

5.2.4.4 Maatregelen voor de gebruiker

De voorgaande maatregelen zijn met name gericht op de aanbodkant van Ambient Networks. Maar ook de gebruiker heeft natuurlijk bepaalde verantwoordelijkheden op beveiligingsgebied.

10. *Bewustwording*: De gebruiker dient bewust te zijn van de beveiligingsrisico's die hij loopt bij het gebruik van zijn middelen in Ambient Networks.
11. *Op de hoogte van wet- en regelgeving raken*: De gebruiker heeft de verantwoordelijkheid op de hoogte te zijn van de wettelijke bepalingen op het gebied van informatiebeveiliging, de bescherming van persoonsgegevens en het doen van transacties op het Internet.
12. *Zorgvuldig gebruik*: De gebruiker dient zorgvuldig om te gaan met de middelen die hij of zij tot zijn of haar beschikking heeft zodra hij of zij diensten afneemt over Ambient Networks. Gevoelige informatie die daarbij vrijkomt dient daarbij voldoende beschermd te worden.

6 Security visie

In dit hoofdstuk geeft TNO zijn visie op security voor Ambient Networks:

1. Allereerst op de verschillende security aspecten (uit paragraaf 5.1) en dat per toekomstscenario.
2. Vervolgens op de maatregelen die aan deze security aspecten gerelateerd zijn (uit paragraaf 5.2). En dat ook weer per scenario, maar dan opgehangen aan de geïdentificeerde partijen (uit paragraaf 3.2) binnen de toekomstige markt voor Ambient Networks.
3. En in enkele slotopmerkingen wordt ingegaan op wat dit voor de beleidsmakers betekent.

6.1 Visie op security aspecten per scenario

Concreet worden in de volgende vier subparagrafen per scenario de, volgens TNO meest relevante, technische en algemene kwetsbaarheden en dreigingen en omgevingsaspecten behandeld. In de vijfde subparagraaf worden de meest voorkomende security aspecten genoemd. Dit zijn de zogenaamde ‘hot issues’ die naar verwachting in vrijwel alle scenario’s voor zullen komen.

6.1.1 Voor het scenario ‘Afwachtend’

Doordat de samenleving is gebaseerd op zekerheid, staat beveiliging relatief hoog in het vaandel. Er wordt gezocht naar goedkope maar veilige oplossingen voor het relatief kleine aanbod van diensten. Voor de grote bedrijven die de economie domineren is het redelijk overzichtelijk wat ze moeten beveiligen en hoe ze dit moeten doen.

De belangrijkste technische kwetsbaarheden en dreigingen (zie paragraaf 5.1.1) in dit scenario zijn hieronder weergegeven. (De niet genoemde kwetsbaarheden en dreigingen zijn volgens TNO minder relevant binnen dit scenario. Hier is uiteraard wel discussie over mogelijk.)

- *Netwerkkoppelingen*: omdat de maatschappij binnen dit scenario steunt op het collectief, zal toegang tot netwerken meestal niet per device, maar per netwerk(domein) geregeld worden. De gebruikers nemen collectief soortgelijke diensten af.
- *De IP verbinding*: voor de gebruiker is het belangrijk dat de dienst, en dus ook de onderliggende IP verbinding, stabiel is. De gebruiker ziet graag ‘end-to-end security’.
- *Compatibiliteit*: doordat er relatief lang op oude systemen zal worden voortborduurd, is het van belang dat nieuwe systemen goed aansluiten op de bestaande infrastructuur.
- *Communicatie binnen groepen*: door de verzuiling is er veel behoefte in communicatie binnen groepen met bijbehorende security oplossingen.

De belangrijkste algemene kwetsbaarheden en dreigingen (zie paragraaf 5.1.2) in dit scenario zijn:

- *Vertrouwen*: in deze samenleving is vertrouwen in Ambient Networks belangrijk. De gebruiker wil niet voor verassingen te komen staan.
- *De digitale kloof*: door de verzuiling van de samenleving is het risico van een digitale kloof tussen ‘jong’ en ‘oud’ (mensen die open staan voor nieuwe technologieën en mensen die dat niet zijn) redelijk hoog.

De belangrijkste omgevingsaspecten (zie paragraaf 5.1.3) in dit scenario zijn:

- *Een toenemende afhankelijkheid van ICT*: door de toenemende afhankelijkheid van ICT en de behoefte aan stabiliteit is er een relatief hoge behoefte aan governance, zowel Europees als nationaal.
- *Professionalisering van cybercrime*: de gebruikers huiveren bij het denken aan cybercrime. De aanbieders in de markt zijn in de positie om hier maatregelen tegen te nemen, maar zij stellen zich afwachtend op.

6.1.2 Voor het scenario 'Bewogen'

Hoewel gebruikers minder belang hechten aan beveiliging, zullen ze wel sneller schakelen tussen het beperkt aantal beschikbare netwerken en diensten waardoor beveiligingsmechanismen ook dynamisch moeten zijn. Er zijn relatief weinig aanbieders, maar doordat gebruikers snel veranderen is beveiliging toch lastig te realiseren.

De belangrijkste technische kwetsbaarheden en dreigingen (zie paragraaf 5.1.1) in dit scenario zijn:

- *Toegang tot netwerken*: de gebruiker zal vaak via onbekende netwerken toegang willen krijgen tot bekende netwerken. De Ambient Networks omgeving moet dit dan ook faciliteren. De aanbodkant in dit scenario doet dit vaak niet.
- *Mobiliteitsmechanismen*: de vraag naar mobiliteitsmechanismen is hoog terwijl de aanbieders hier vaak niet op berekend zijn en dus is de kans op misbruik hiervan ook relatief hoog.
- *De fysieke verbinding*: doordat gebruikers vaak wisselen tussen de verschillende domeinen en netwerken, is de kwaliteit van de fysieke verbinding een aandachtspunt. Bij een uniform aanbod is de verwachting dat dit voor het beperkte aanbod van netwerken wel goed op elkaar is afgestemd.
- *Compatibiliteit*: een aanbod van nieuwe netwerken zal beperkt zijn, maar de vraag is divers, dus er is een hoge behoefte aan compatibiliteit tussen de oude en de nieuwe systemen.

De belangrijkste algemene kwetsbaarheden en dreigingen (zie paragraaf 5.1.2) in dit scenario zijn:

- *Privacy*: gebruikers zijn minder privacy bewust hoewel ze wel veel gebruik maken van nieuwe diensten met het gevaar dat persoonsgegevens 'op straat' komen.
- *De digitale kloof*: het gevaar is dat er een kloof ontstaat tussen de gebruikers die snel kunnen schakelen in de digitale wereld en de rest van de bevolking die dat niet kan of wil.

De belangrijkste omgevingsaspecten (zie paragraaf 5.1.3) in dit scenario zijn:

- *Een toenemende afhankelijkheid van ICT*: doordat gebruikers in toenemende mate zich afhankelijker maken van ICT, waarbij het aanbod overzichtelijk is, blijkt zich een behoefte aan regulering op nationaal niveau te ontwikkelen.
- *Gebrek aan beveiligingsbewustzijn bij gebruikers*: de gebruikers binnen dit scenario zijn zich niet bewust van de gevaren die de moderne technologieën met zich meebrengen. De aanbieders en de overheid hebben hier een opvoedende rol.

6.1.3 Voor het scenario 'Complex'

Het grote aanbod in de markt en de variërende vraag van de gebruikers maakt beveiliging in dit scenario uitermate lastig. De maatschappij vraagt om flexibele

beveiligingsmechanismen die dynamisch op de behoefte van de gebruiker kunnen inspelen. De aanbodkant is vooral gericht op innovatie en minder op security.

De belangrijkste technische kwetsbaarheden en dreigingen (zie paragraaf 5.1.1) in dit scenario zijn:

- *Toegang tot netwerken*: toegang tot onbekende netwerken of via netwerken zonder registratie vooraf is aan de orde van de dag.
- *Mobiliteitsmechanismen*: de snelle schakeling van gebruikers vraagt om goede mobiliteitsmechanismen en stelt hoge eisen aan de beveiliging daarvan.
- *De IP verbinding*: ook in het IP domein zal snel en vaak tussen verschillende domeinen geschakeld worden wat end-to-end security in de weg kan staan.
- *De fysieke verbinding*: de gebruikers schakelen snel tussen netwerken van verschillende aanbieders waardoor de stabiliteit van de fysieke verbinding in het gedrang komt.
- *Beheer en autorisatie*: de veelheid aan devices vraagt om aandacht voor het beheer daarvan en het managen van de autorisaties.
- *Compatibiliteit*: de veelheid aan (mogelijk verouderde) systemen maakt compatibiliteit ertussen van belang.
- *Gebruik van context informatie*: door gebruik te maken van context informatie (welke devices heeft ene gebruiker en welke diensten gebruikt hij of zij) kan beter worden ingespeeld op de (beveiligings)behoefte van de gebruiker.

De belangrijkste algemene kwetsbaarheden en dreigingen (zie paragraaf 5.1.2) in dit scenario zijn:

- *Vertrouwen*: met name in een snel wisselende maatschappij is het opbouwen van vertrouwen lastig en zullen de beveiligingsmechanismen hieraan moeten worden aangepast.
- *Technische complexiteit*: in deze uiterst complexe en dynamische omgeving (zowel de vraag als aanbodkant) is het lastig om de juiste en gebruiksvriendelijke security mechanismen op te tuigen.
- *Privacy*: de aanwezigheid van veel gebruikers die zich bij veel verschillende diensten registreren verhoogt de kans op misbruik van privacy.
- *Identiteitsmanagement*: binnen elk domein zal een gebruiker een andere identiteit hebben. Door de grote diversiteit van het aanbod wordt het managen van die identiteiten van belang.

De belangrijkste omgevingsaspecten (zie paragraaf 5.1.3) in dit scenario zijn:

- *Een gefragmenteerde omgeving*: de veelheid aan partijen maakt de markt onoverzichtelijk, waarbij verantwoordelijkheden helder moeten worden neergelegd.
- *Gebrek aan beveiligingsbewustzijn bij gebruikers*: de gebruikers binnen dit scenario zijn zich niet bewust van de gevaren van de alledaagse technologieën met zich meebrengen. De aanbieders zijn vooral bezig met verdere ontwikkeling en hebben voor security minder oog.

6.1.4 Voor het scenario ‘Degelijk’

De beveiligingsbehoefte van de gebruiker verandert weinig en is relatief duidelijk. Hoewel er vele aanbieders zijn, zijn er via de vaste winkelformules en marktbenaderingen toch goede mogelijkheden om de beveiliging op orde te krijgen.

De belangrijkste technische kwetsbaarheden en dreigingen (zie paragraaf 5.1.1) in dit scenario zijn:

- *Toegang tot netwerken*: doordat het beperkt aantal gebruikte diensten via verschillende aanbieders en netwerken lopen, is toegang tot deze netwerken een aandachtspunt.
- *Netwerkkoppelingen*: doordat veel devices met dezelfde netwerken zullen willen worden gekoppeld is het handig om deze koppelingen op netwerkniveau te regelen.
- *Compatibiliteit*: gebruikers willen oude infrastructuren blijven gebruiken dus compatibiliteit van nieuwe netwerken met de oude infrastructuren is noodzakelijk. De aanbodkant zit hier echter niet op te wachten.

De belangrijkste algemene kwetsbaarheden en dreigingen (zie paragraaf 5.1.2) in dit scenario zijn:

- *Privacy*: doordat de gegevens van de gebruikers bij veel verschillende aanbieders bekend zijn, waarvan de gebruikers niet op de hoogte zijn, is bescherming van de privacy geboden.
- *Identiteitsmanagement*: diensten zullen veelal gekoppeld over verschillende domeinen aan de gebruker worden aangeboden. Binnen elk domein heeft een gebruiker echter een andere identiteit. Dat maakt het beheer van deze identiteiten een belangrijk aandachtspunt.
- *De digitale kloof*: in deze samenleving geldt: als je niet meekomt in de digitale wereld lig je er al snel uit.

De belangrijkste omgevingsaspecten (zie paragraaf 5.1.3) in dit scenario zijn:

- *Een gefragmenteerde omgeving*: de diversiteit van het aanbod zorgt voor onduidelijkheid in de verantwoordelijkheid en aansprakelijkheid.
- *Professionalisering van cybercrime*: de maatschappij is weinig beveiligingsbewust en het aanbod van ICT diensten is hoog waardoor het voor criminelen interessanter wordt om misbruik te gaan maken van deze diensten.
- *Gebrek aan beveiligingsbewustzijn bij gebruikers*: de gebruikers binnen dit scenario zijn zich totaal niet bewust van de gevaren die de overvloed aan moderne technologieën met zich meebrengen. Ook hier zijn de aanbieders vooral bezig met verdere ontwikkeling en hebben ze voor security minder oog.

6.1.5 De meest voorkomende security aspecten (‘hot issues’)

De security aspecten die in tenminste drie van de vier scenario’s voorkomen zijn:

1. Compatibiliteit
2. Privacy
3. De digitale kloof
4. Gebrek aan beveiligingsbewustzijn bij gebruikers

Uit de analyse volgt dat deze onderwerpen van belang zullen zijn in alle vier de mogelijke toekomstscenario’s. Hoewel dat geen garantie is dat deze onderwerpen daadwerkelijk een dergelijke rol zullen spelen in de toekomst, zijn dit wel de onderwerpen die prioriteit zouden moeten krijgen op het moment dat marktpartijen en de overheid zich willen voorbereiden op de ontwikkeling van Ambient Networks.

6.2 Visie op beveiligingsmaatregelen per scenario

Bij de hierboven genoemde security aspecten horen vanzelfsprekend maatregelen, zoals genoemd in paragraaf 5.2. Deze zullen moeten worden uitgevoerd door de verschillende partijen uit de paragrafen 3.1 en 3.2. In onderstaande tabellen is dit per scenario samengevat.

Tabel 6.1: Wie voert welke maatregelen uit binnen het scenario Afwachtend?

Kwetsbaarheid of dreiging (§ 5.1)	Belangrijkste maatregel (§ 5.2.1 – 5.2.3)	Uitvoerende partij (§ 3.1 en 3.2)
Netwerkkoppelingen	technische protocollen implementeren en naleven	netwerk operators en fabrikanten
De IP verbinding	kennis opdoen over hoe hier mee om te gaan	netwerk operators, service providers en fabrikanten
Compatibiliteit	oude systemen ondersteunen	netwerk operators en fabrikanten
Communicatie binnen groepen	n.v.t.	netwerk operators, service providers en fabrikanten
Vertrouwen	toepassen van elektronische certificaten	netwerk operators en service providers
De digitale kloof	de zwakke groep beschermen	overheid
Een toenemende afhankelijkheid van ICT	meer controle over de beveiligingsprocessen	netwerk operators, service providers en fabrikanten
Professionalisering van cybercrime	meer preventie, opsporing en vervolging	overheid
	Aanvullende maatregelen (§ 5.2.4)	
	kennis op peil houden	netwerk operators, service providers en fabrikanten

Tabel 6.2: Wie voert welke maatregelen uit binnen het scenario Bewogen?

Kwetsbaarheid of dreiging (§ 5.1)	Belangrijkste maatregel (§ 5.2.1 – 5.2.3)	Uitvoerende partij (§ 3.1 en 3.2)
Toegang tot netwerken	toegang moet procedureel op orde zijn	netwerk operators
Mobiliteitsmechanismen	fraudescenario's inventariseren en maatregelen treffen	netwerk operators en service providers
De fysieke verbinding	technische protocollen implementeren en naleven	fabrikanten
Compatibiliteit	oude systemen ondersteunen	netwerk operators en fabrikanten
Privacy	wet- en regelgeving opstellen en naleven	netwerk operators, service providers en de overheid
De digitale kloof	de zwakke groep beschermen	overheid
Een toenemende afhankelijkheid van ICT	meer controle over de beveiligingsprocessen	netwerk operators, service providers en fabrikanten
Gebrek aan beveiligingsbewustzijn bij gebruikers	voorlichting	overheid en service providers
	Aanvullende maatregelen (§ 5.2.4)	
	toepassing van pseudoniemen	netwerk operators en service providers
	kennis op peil houden	netwerk operators, service providers en fabrikanten

	wet- en regelgeving toekomst-bestendig maken	overheid
	digitale territorium	service providers
	controle over persoonlijke infor-matie voor de gebruiker	netwerk operators en service providers
	bewustwording	gebruiker
	op de hoogte van wet- en regel-geving raken	gebruiker
	zorgvuldig gebruik	gebruiker

Tabel 6.3: Wie voert welke maatregelen uit binnen het scenario Complex?

Kwetsbaarheid of dreiging (§ 5.1)	**Belangrijkste maatregel (§ 5.2.1 – 5.2.3)**	**Uitvoerende partij (§ 3.1 en 3.2)**
Toegang tot netwerken	toegang moet procedureel op orde zijn	netwerk operators
Mobiliteitsmechanismen	fraudescenario's inventariseren en maatregelen treffen	netwerk operators en service providers
De IP verbinding	kennis opdoen over hoe hier mee om te gaan	netwerk operators, service pro-viders en fabrikanten
De fysieke verbinding	technische protocollen imple-menteren en naleven	fabrikanten
Beheer en autorisatie van mid-delen	beheren: eigenaar toewijzen en rollen definiëren	netwerk operators en service providers
Compatibiliteit	oude systemen ondersteunen	netwerk operators en fabrikan-ten
Gebruik van context informatie	n.v.t.	service providers
Vertrouwen	toepassen van elektronische certificaten	netwerk operators en service providers
Technische complexiteit	beheer decentraal inrichten	netwerk operators en service providers
Privacy	wet- en regelgeving opstellen en naleven	netwerk operators, service pro-viders en de overheid
Identiteitsmanagement	identiteitsmanagementsysteem implementeren	netwerk operators en service providers
Een gefragmenteerde omgeving	verantwoordelijkheden helder maken	netwerk operators, service pro-viders en de overheid
Gebrek aan beveiligingsbewust-zijn bij gebruikers	voorlichting	overheid en service providers
	Aanvullende maatregelen (§ 5.2.4)	
	opslag van persoonsgegevens minimaliseren	netwerk operators en service providers
	veilige autorisatie	netwerk operators en service providers
	toepassing van pseudoniemen	netwerk operators en service providers
	stimuleren van open standaar-den	netwerk operators, service pro-viders en de overheid

	keurmerken t.b.v. vertrouwen	netwerk operators, service providers en de overheid
	wet- en regelgeving toekomstbestendig maken	overheid
	digitale territorium	service providers
	controle over persoonlijke informatie voor de gebruiker	netwerk operators en service providers
	bewustwording	gebruiker
	op de hoogte van wet- en regelgeving raken	gebruiker
	zorgvuldig gebruik	gebruiker

Tabel 6.4: Wie voert welke maatregelen uit binnen het scenario Degelijk?

Kwetsbaarheid of dreiging (§ 5.1)	**Belangrijkste maatregel (§ 5.2.1 – 5.2.3)**	**Uitvoerende partij (§ 3.1 en 3.2)**
Toegang tot netwerken	toegang moet procedureel op orde zijn	netwerk operators
Netwerkkoppelingen	technische protocollen implementeren en naleven	netwerk operators en fabrikanten
Compatibiliteit	oude systemen ondersteunen	netwerk operators en fabrikanten
Privacy	wet- en regelgeving opstellen en naleven	netwerk operators, service providers en de overheid
Identiteitsmanagement	identiteitsmanagementsysteem implementeren	netwerk operators en service providers
De digitale kloof	de zwakke groep beschermen	overheid
Een gefragmenteerde omgeving	verantwoordelijkheden helder maken	netwerk operators, service providers en de overheid
Professionalisering van cybercrime	meer preventie, opsporing en vervolging	overheid
Gebrek aan beveiligingsbewustzijn bij gebruikers	voorlichting	overheid en service providers
	Aanvullende maatregelen (§ 5.2.4)	
	opslag van persoonsgegevens minimaliseren	netwerk operators en service providers
	toepassing van pseudoniemen	netwerk operators en service providers
	stimuleren van open standaarden	netwerk operators, service providers en de overheid
	kennis op peil houden	netwerk operators, service providers en fabrikanten
	wet- en regelgeving toekomstbestendig maken	overheid
	digitale territorium	service providers
	controle over persoonlijke informatie voor de gebruiker	netwerk operators en service providers
	bewustwording	gebruiker

	op de hoogte van wet- en regelgeving raken	gebruiker
	zorgvuldig gebruik	gebruiker

6.2.1 Voor de 'hot issues'

Bij de eerder genoemde 'hot issues' (in subparagraaf 6.1.5) horen ook maatregelen. Deze zijn in dit geval toegespitst op de overheid en worden per scenario behandeld.

1.) Compatibiliteit

A. Scenario Afwachtend: De overheid kan een paar grote bedrijven stimuleren om compatibel te blijven met bestaande systemen.
B. Scenario Bewogen: Door de dynamische vraag zal de markt het hier misschien eerder vanzelf oppakken. Toch dienst de overheid grote bedrijven licht te stimuleren.
C. Scenario Complex: Dit is moeilijk aan te sturen door de overheid. De overheid kan beter de gebruikers bewust maken van het compatibiliteitsaspect bij hun keuze.
D. Scenario Degelijk: De aanbieders zitten waarschijnlijk niet te wachten op sturing door de overheid dus wellicht is wettelijke regulering hier meer geschikt als stuurinstrument dan bewustwording bij de aanbieders.

2.) Privacy

B. Scenario Bewogen: De gebruikers binnen dit scenario willen veel Ambient Networks diensten gebruiken, maar ze zijn zich nog niet bewust van de gevaren rondom privacy. De belangrijkste taak van de overheid ligt dan ook in het privacy bewust maken van de gebruiker.
C. Scenario Complex: De overheid dient de gebruiker bewust te maken van zijn privacy en daarnaast voorlichting te geven over hoe gebruikers met persoonsgegevens moeten omgaan. Daarnaast dient de overheid de aanbieders te stimuleren om gebruikers op de juiste wijze met persoonsgegevens om te laten gaan. Een optie is ook het uitgeven van privacykeurmerken zodat aanbieders zich hiermee kunnen onderscheiden.
D. Scenario Degelijk: De overheid dient de gebruiker bewust te maken zodat privacy onderdeel wordt van de gebruikersbehoefte ten aanzien van de afname van Ambient Networks diensten.

3.) De digitale kloof

A. Scenario Afwachtend: Omdat de ontwikkelingen niet zo hard gaan is de digitale kloof hier relatief eenvoudig te beperken. De (weinige) diensten moeten zoveel mogelijk toegankelijk en gebruikersvriendelijk worden gemaakt zodat alle delen van de samenleving kunnen meeprofiteren.
B. Scenario Bewogen: Hier is het gevaar wat groter omdat de vraag dynamischer is dan het aanbod dus is het moeilijker bij te houden voor digibeten. Naast de maatregelen uit het scenario Afwachtend kan de overheid voorlichting geven om duidelijk te maken wat je met bepaalde diensten kunt doen zodat digibeten minder worden afgeleid door de dynamiek van hun technische medemens.
D. Scenario Degelijk: In dit scenario geldt een relatief hoog risico op een digitale kloof. Het uitgebreide aanbod dient zo toegankelijk en gebruikersvriendelijk mogelijk te worden gemaakt. De overheid kan eventueel subsidies uitschrijven aan service providers hiervoor. De voorlichting dient duidelijkheid te geven over het

diverse aanbod aan diensten. Eventueel is regelgeving mogelijk om transparantie in de markt te bevorderen.

4.) Gebrek aan beveiligingsbewustzijn bij gebruikers

B. Scenario Bewogen: De gebruikers binnen dit scenario willen veel Ambient Networks diensten gebruiken, maar ze zijn zich nog niet bewust van de algemene gevaren. De belangrijkste taak van de overheid ligt dan ook in het veiligheidsbewust maken van de gebruiker.
C. Scenario Complex: De overheid dient de gebruiker bewust te maken van de risico's in de digitale wereld en daarnaast voorlichting te geven over hoe gebruikers bepaalde (‘best practice’) maatregelen kunnen nemen. Daarnaast dient de overheid de aanbieders te stimuleren om de gebruiker te attenderen op beveiligingsriskante acties door de gebruikers zo duidelijk mogelijke meldingen te geven.
D. Scenario Degelijk: De overheid kan de gebruiker bewustmaken van zijn digitale territorium zodat beveiliging een onderdeel wordt van zijn vaste behoefte.

6.3 Slotopmerkingen

In deze paragraaf volgen nog enkele slotopmerkingen naar aanleiding van de paragrafen 6.1 en 6.2. Want nu de verschillende scenario’s voor de toekomstige markt voor Ambient Networks zijn geschetst, vervolgens bekeken is welke security aspecten met name kunnen spelen binnen deze scenario’s en welke maatregelen welke partij binnen de toekomstige markt daartegen zou kunnen nemen, volgen hier nog een paar slotopmerkingen.

6.3.1 Over welk scenario het gaat worden (en waarom)

Nu, december 2006, kent de aanbodkant van de huidige ICT-markt een brede uitrol van gecombineerde bel- en Internetdiensten. Weliswaar zijn dit geen Ambient Networks diensten, maar het is niet onvoorstelbaar dat, wanneer Ambient Networks diensten gemeengoed worden, de aanbodkant zich net zo zal gaan gedragen als nu het geval is met deze innovatieve diensten. Ook de vraagkant is gretig gezien de onverwacht grote afname van deze nieuwe diensten. De consument is absoluut niet te typeren als afwachtend. Dus zowel de vraag- als aanbodkant is te typeren als min of meer ‘gretig’. Het meest waarschijnlijke scenario is dan het **scenario ‘Complex’**. Het minst waarschijnlijke scenario is dan het scenario ‘Afwachtend’. Het is echter moeilijk te voorspellen of de aanbodkant zo divers zal blijven de komende jaren als die nu is. De strijd tussen telecom operators en kabelaars is in volle gang en het is nog onduidelijk hoe de overgang van dual play naar triple play (bellen, Internet en digitale TV) zal verlopen. En wellicht zullen de consumenten ook wat afwachtender worden op het moment dat de economische situatie verandert.

6.3.2 Over centrale versus decentrale besturing (van security)

Vanwege de verwachte complexiteit (binnen het scenario Complex) zal de aanbodkant het beheer van de netwerken en diensten in grote lijnen decentraal gaan inrichten. Bij een zeer divers aanbod en een uiterst dynamische vraag ontstaat namelijk een buitengewoon complex geheel van vraag en aanbod naar netwerken en diensten. Het beheer is hierom slecht centraal uit te voeren omdat alle beheerinformatie in grote hoeveelheden erg onsamenhangend beschikbaar komt. Dit maakt (met name het technische) beheer complex.

Ten aanzien van security is dit niet anders. Security zal decentraal (lokaal) moeten worden geïmplementeerd waarbij de aanbieders van de netwerken en diensten (netwerk

operators en service providers) op centraal niveau high-level beveiligingsmaatregelen invoeren. Concreet betekent dit dat decentraal technische (best practice) beveiligingsmaatregelen worden getroffen en op centraal niveau men meer beleidsmatige beveiligingsmaatregelen treft.

6.3.3 Over 'blinde vlekken (waar de overheid vrijwel niet op kan sturen)

In de toekomstige markt verwacht TNO een aantal blinde vlekken waar de overheid vrijwel niet of slecht op kan sturen. Deze blinde vlekken kunnen een negatieve invloed hebben op de security van Ambient Networks. Hierbij valt te denken aan:

1. *De eerste implementaties van technieken en diensten*. De eerste implementaties van bijvoorbeeld WiFi destijds bleken erg onveilig. Op dit moment kan de overheid slechte implementaties vrijwel niet voor zijn. Hoogstens kan men bij de aanbieders sturen op de naleving van internationale technische protocollen waar security goed in is meegenomen. Regulering in een vroegtijdig stadium is vaak ook nadelig voor het innovatieve karakter van een nieuwe technologie.
2. *Herkomst bepalen van aanvallen via Internet.* Omdat aanvallen via Internet vaak via talloze schakels kunnen lopen over verschillende landen met ieder hun eigen wetgeving is dit een lastige kwestie. Enerzijds is het moeilijk om de herkomst te bepalen en anderzijds is het gecompliceerd om hier wetgeving over te maken, de aanvaller zal zijn aanval initiëren vanuit het land met de voor hem meest gunstige wetgeving.

6.3.4 Over de gebruiker in de toekomstige markt (vraagkant)

Gebruikers worden steeds afhankelijker van ICT. Daarnaast worden ze ook steeds onwetender (men weet niet meer hoe het in elkaar steekt). De techniek wordt steeds abstracter en is voor de gebruiker puur functioneel waarbij hij geen idee meer heeft hoe het daadwerkelijk werkt. Het gebruik van de techniek vindt plaats op basis van vertrouwen, de digitale kloof tussen de digibeten en de (intensieve) ICT-gebruikers zal waarschijnlijk groeien. Daarnaast worden de gebruikers steeds veeleisender (vooral in het scenario Complex) en zullen zij diensten over diensten heen gebruiken.

6.3.5 Over de partijen in de toekomstige mark (aanbodkant)

Zoals al gezegd in paragraaf 3.2, kan een partij meerdere rollen spelen. Bijvoorbeeld netwerk operators en service providers (denk bijvoorbeeld aan partijen die naast een netwerk ook diensten aanbieden). Hierdoor worden verantwoordelijkheden en aansprakelijkheden steeds minder inzichtelijk. Maar ook door de veelheid aan partijen wordt het er allemaal niet duidelijker op. Zo kan een dienst van een service provider met een device van een fabrikant over een netwerk van een netwerk operator heen wordt gebruikt. Wie is dan verantwoordelijk en/of aansprakelijk voor security?

6.3.6 Over een aanspreekpunt voor de overheid

Wie of wat is het aanspreekpunt voor security voor de overheid? Dit kan verschillen per scenario. Bij een uniform aanbod (de scenario's 'Afwachtend' en 'Bewogen') zijn de partijen vaak duidelijk en is het aanspreekpunt voor de overheid dan ook vaak duidelijk. Bij een divers aanbod wordt dit lastiger. Veelal organiseert de overheid zelf al een overleg waar aanbieders van vitale ICT- diensten aanschuiven[31]. Wanneer partijen meerdere rollen spelen en/of deze rollen vervagen wordt het lastig om de juiste partijen aan tafel te krijgen. Binnen een Complex scenario moet er wellicht een herdefiniëring van dit aanspreekpunt plaatsvinden. Hier moeten de fabrikanten ook in vertegenwoordigd zijn.

[31] Zoals het 'NCO-T' (Nationaal COntinuïteitsoverleg Telecommunicatie).

6.3.7 Over reguleren versus een vrije markt

De overheid wil niet alles tot in detail reguleren en dit is zeker binnen een Complex scenario ook af te raden omdat de overheid de complexe markt (van dynamische vraag en divers aanbod) niet bij moet willen houden. De markt kan beter ‘vrij worden gelaten’. Concreet betekent dit binnen een Complex scenario dat de overheid de markt zelf laat innoveren en alleen beperkt bijstuurt wanneer de markt ‘onveilig’ wordt voor de gebruiker (wanneer bijvoorbeeld diens privacy in het geding is). In een Afwachtend scenario echter zijn er meer mogelijkheden voor de overheid om de markt te reguleren. De markt is minder in beweging en daarom beter voorspelbaar en de consumenten hebben ook hogere verwachtingen ten aanzien van regulering.

7 Conclusies en aanbevelingen

In dit hoofdstuk volgen de conclusies en aanbevelingen naar aanleiding van dit onderzoek.

7.1 Conclusies

De volgende algemene conclusies zijn te trekken:

1. Dit onderzoek geeft inzicht in de security aspecten (paragraaf 5.1) en de maatregelen die je daar tegen kunt nemen (paragraaf 5.2) van de toekomstige Nederlandse markt voor Ambient Networks.
2. De meest voorkomende security aspecten binnen de vier scenario's zijn; *compatibiliteit* van 'oude' technieken en devices met de nieuwe techniek; de *privacy* van gebruikers die dikwijls in het geding komt; *de digitale kloof* die kan ontstaan tussen personen die mee kunnen en willen gaan met nieuwe ontwikkelingen in de ICT en personen die dat niet kunnen of willen; en een *gebrek aan beveiligingsbewustzijn bij gebruikers*.
3. In de toekomstige markt voor Ambient Networks verwacht TNO de volgende 'blinde vlekken' waar de overheid beperkt op kan sturen; (1) *de eerste implementaties van nieuwe technieken en diensten*; en (2) de *herkomst bepalen van aanvallen via Internet*.
4. Bij drie van de vier scenario's blijkt dat de gebruikers steeds afhankelijker worden van ICT en dat ze er steeds minder van zullen gaan weten.
5. In het algemeen zullen de rollen van de netwerk operators en service providers meer en meer vervagen waardoor de verantwoordelijkheid en aansprakelijkheid voor security steeds minder inzichtelijk wordt. (Het aanspreekpunt voor de overheid is hierdoor ook aan verandering onderhevig, maar dat verschilt per scenario.)

7.2 Aanbevelingen

Hier volgen enkele algemene aanbevelingen die onafhankelijk zijn van het beschouwde toekomstscenario.

7.2.1 Algemene aanbevelingen

1. De overheid dient kennis te nemen van de meest voorkomende security aspecten (hot issues) die zullen gaan spelen binnen de toekomstige markt voor Ambient Networks (paragrafen 6.1.5 en 5.1) en de maatregelen die je daar tegen kunt nemen (paragraaf 5.2).
2. Op basis hiervan dient de overheid alvast stelling te nemen ten aanzien van deze toekomstige kwesties. Wellicht dat hier nog onderzoek naar specifieke kwesties aan vooraf zou moeten gaan.
3. Compatibiliteit met oude systemen blijkt in alle scenario's een belangrijk issue. De overheid dient beleid voor te bereiden om compatibiliteit onder de aandacht te brengen bij aanbieders en om gebruikers bewust te maken van dit aspect.
4. Daarnaast kan de overheid de markt monitoren op welk scenario gaat spelen in de toekomst. Wordt de aanbodkant meer divers of juist uniformer? En de vraagkant, wordt deze dynamischer of juist statischer?

Hierna volgen per scenario steeds vijf aanbevelingen;

- de eerste gaat over het aanspreekpunt voor de overheid;
- de tweede over of de overheid de markt zal reguleren of dat de overheid juist in staat is om de markt vrij te laten;
- de derde over welke rol de overheid zich aan kan meten;
- de vierde over welke variabelen de overheid op kan monitoren;
- en de vijfde gaat over welke maatregelen de overheid kan nemen tegen de meest voorkomende security aspecten binnen het betreffende scenario.

7.2.2 Voor het scenario 'Afwachtend'

1. De overheid kan in dit scenario het beste contacten leggen met de centrale netwerk operator als zijnde het aanspreekpunt en/of stuurinstrument.
2. In dit scenario kan de overheid veel security kwesties reguleren omdat zowel de vraag- als aanbodkant van de markt een afwachtende houding aannemen. Zaken op hun beloop laten (de markt vrijlaten) heeft weinig zin omdat de markt weinig initiatief toont.
3. De overheid kan zich in dit scenario zowel voor de uniforme aanbodkant als de statische vraagkant een stimulerende rol aanmeten om eventueel de markt in zijn geheel te stimuleren tot actieve beveiliging van de beperkte Ambient Networks markt.
4. De overheid kan binnen dit scenario monitoren op de variabelen:
    - beveiligingsniveau van de aangeboden diensten en netwerken

   …om de uniforme aanbodkant te stimuleren en daarnaast ook monitoren op:
    - het beveiligingsbewustzijn bij de gebruikers

   …om ook de statische vraagkant te stimuleren.
5. De overheid kan voor dit scenario de volgende maatregelen voor de 'hot issues' overwegen:
    - Compatibiliteit - De overheid kan een paar grote bedrijven stimuleren om compatibel te blijven met bestaande systemen.
    - De digitale kloof - Omdat de ontwikkelingen niet zo hard gaan is de digitale kloof hier relatief eenvoudig te beperken. De (weinige) diensten moeten zoveel mogelijk toegankelijk en gebruikersvriendelijk worden gemaakt zodat alle delen van de samenleving kunnen meeprofiteren.

7.2.3 Voor het scenario 'Bewogen'

1. De overheid kan in dit scenario het beste contacten leggen met de belangrijkste netwerk operator als zijnde het aanspreekpunt en/of stuurinstrument.
2. In dit scenario is de aanbodkant uniform terwijl de vraag dynamisch is. De overheid kan hierom wellicht de aanbodkant stimuleren (reguleren) om meer aanbod te creëren terwijl men de vraagkant vrij laat.
3. De overheid kan zich in dit scenario met name een stimulerende rol aanmeten ten aanzien van de uniforme aanbodkant en een wakende rol ten aanzien van de dynamische vraagkant (de gebruikers) om zo te sturen op een veilige markt voor Ambient Networks.
4. De overheid kan binnen dit scenario monitoren op de variabelen:
    - het beveiligingsniveau van de aangeboden diensten en netwerken

   …om de uniforme aanbodkant te stimuleren en daarnaast ook monitoren op:
    - het aantal gebruikers van per dienst
    - het aantal afgenomen diensten
    - het aantal gebruikt netwerken
    - het gebruik van deze netwerken en diensten (kwalitatief)
    - het type incidenten (en of ze structureel zijn)
    - het beveiligingsbewustzijn bij de gebruikers

…om de dynamische vraagkant te bewaken.

5. De overheid kan voor dit scenario de volgende maatregelen voor de ‘hot issues’ overwegen:
    - Compatibiliteit - Door de dynamische vraag zal de markt het hier misschien eerder vanzelf oppakken. Toch dienst de overheid grote bedrijven licht te stimuleren.
    - Privacy - De gebruikers binnen dit scenario willen veel Ambient Networks diensten gebruiken, maar ze zijn zich nog niet bewust van de gevaren rondom privacy. De belangrijkste taak van de overheid ligt dan ook in het privacy bewust maken van de gebruiker.
    - De digitale kloof - Hier is het gevaar wat groter dan bij het scenario Afwachtend omdat de vraag dynamischer is en digibeten het dus moeilijker hebben om hun technische omgeving bij te benen. Naast de maatregelen uit het scenario Afwachtend kan de overheid voorlichting geven om duidelijk te maken wat je met bepaalde diensten kunt doen zodat digibeten minder worden afgeleid door de dynamiek van hun technische medemens.
    - Gebrek aan beveiligingsbewustzijn bij gebruikers - De gebruikers binnen dit scenario willen veel Ambient Networks diensten gebruiken, maar ze zijn zich nog niet bewust van de algemene gevaren. De belangrijkste taak van de overheid ligt dan ook in het veiligheidsbewust maken van de gebruiker.

7.2.4 Voor het scenario ’Complex’

1. De overheid kan in dit scenario het beste contacten leggen met een vertegenwoordiging van de belangrijkste netwerk operators en service providers als zijnde het centrale aanspreekpunt en/of stuurinstrument.
2. In dit scenario is de vraag- en aanbodkant respectievelijk dynamisch en divers. Van beide kanten is men actief met het aanbieden en afnemen van diensten wat zorgt voor een complexe, technologische, lastig te beheren infrastructuur. De overheid doet er verstandig aan dit niet tot in detail te willen reguleren. Men kan de markt beter vrijlaten.
3. De overheid kan zich in dit scenario zowel voor de diverse aanbodkant als de dynamische vraagkant een wakende rol aanmeten om eventueel de markt in zijn geheel te bewaken en zo te kunnen sturen op actieve beveiliging van de ‘overspannen’ Ambient Networks markt.
4. De overheid kan binnen dit scenario monitoren op de variabelen:
    - het aantal aanbieders van diensten en netwerken
    - het aantal aangeboden diensten
    - het aantal aangeboden netwerken
    - het beveiligingsniveau van de aangeboden diensten en netwerken

    …om de diverse aanbodkant te bewaken en daarnaast ook monitoren op:
    - het aantal gebruikers van per dienst
    - het aantal afgenomen diensten
    - het aantal gebruikt netwerken
    - het gebruik van deze netwerken en diensten (kwalitatief)
    - het type incidenten (en of ze structureel zijn)
    - het beveiligingsbewustzijn bij de gebruikers

    …om de dynamische vraagkant te bewaken.
5. De overheid kan voor dit scenario de volgende maatregelen voor de ‘hot issues’ overwegen:
    - Compatibiliteit - Dit is moeilijk aan te sturen door de overheid. De overheid kan beter de gebruikers bewust maken van het compatibiliteitsaspect bij hun keuze.

- Privacy - De overheid dient de gebruiker bewust te maken van zijn privacy en daarnaast voorlichting te geven over hoe gebruikers met persoonsgegevens moeten omgaan. Daarnaast dient de overheid de aanbieders te stimuleren om gebruikers op de juiste wijze met persoonsgegevens om te laten gaan. Een optie is ook het uitgeven van privacykeurmerken zodat aanbieders zich hiermee kunnen onderscheiden.
- Gebrek aan beveiligingsbewustzijn bij gebruikers - De overheid dient de gebruiker bewust te maken van de risico's in de digitale wereld en daarnaast voorlichting te geven over hoe gebruikers bepaalde (‘best practice’) maatregelen kunnen nemen. Daarnaast dient de overheid de aanbieders te stimuleren om de gebruiker te attenderen op beveiligingsriskante acties door de gebruikers zo duidelijk mogelijke meldingen te geven.

7.2.5 Voor het scenario ‘Degelijk’

1. De overheid kan in dit scenario het beste contacten leggen met een vertegenwoordiging van de belangrijkste netwerk operators en service providers als zijnde het centrale aanspreekpunt en/of stuurinstrument.
2. In dit scenario kan de overheid het beste het diverse aanbod vrijlaten, terwijl men de statische vraagkant (gebruikers) wellicht voorzichtig kan stimuleren tot een actievere afname van diensten.
3. De overheid kan zich in dit scenario met name een wakende rol aanmeten ten aanzien van de diverse aanbodkant en een stimulerende rol ten aanzien van de statische vraagkant (de gebruikers) om zo te sturen op een veilige markt voor Ambient Networks.
4. De overheid kan binnen dit scenario monitoren op de variabelen:
   - het aantal aanbieders van diensten en netwerken
   - het aantal aangeboden diensten
   - het aantal aangeboden netwerken
   - het beveiligingsniveau van de aangeboden diensten en netwerken

   …om de diverse aanbodkant te bewaken en daarnaast ook monitoren op:
   - het beveiligingsbewustzijn bij de gebruikers

   …om de statische vraagkant te stimuleren.
5. De overheid kan voor dit scenario de volgende maatregelen voor de ‘hot issues’ overwegen:
   - Compatibiliteit - De aanbieders zitten waarschijnlijk niet te wachten op sturing door de overheid dus wellicht is wettelijke regulering hier meer geschikt als stuurinstrument dan bewustwording bij de aanbieders.
   - Privacy - De overheid dient de gebruiker bewust te maken zodat privacy onderdeel wordt van de gebruikersbehoefte ten aanzien van de afname van Ambient Networks diensten.
   - De digitale kloof - In dit scenario geldt een relatief hoog risico op een digitale kloof. Het uitgebreide aanbod dient zo toegankelijk en gebruikersvriendelijk mogelijk te worden gemaakt. De overheid kan eventueel subsidies uitschrijven aan service providers hiervoor. De voorlichting dient duidelijkheid te geven over het diverse aanbod aan diensten. Eventueel is regelgeving mogelijk om transparantie in de markt te bevorderen.
   - Gebrek aan beveiligingsbewustzijn bij gebruikers - De overheid kan de gebruiker bewustmaken van zijn digitale territorium zodat beveiliging een onderdeel wordt van zijn vaste behoefte.

8 Literatuur en referenties

1. IST Advisory Group (2003). *Ambient Intelligence - from vision to reality*, ftp://ftp.cordis.lu/pub/ist/docs/istag-ist2003_draft_consolidated_report.pdf.
2. Overbeek, P. (2000). *Informatiebeveiliging onder controle*, Pearson Education Uitgeverij BV, Amsterdam.
3. Fledderus, E. (2005). *RATIO: de scenario's - beschrijving scenario's (17 mei 2005)*, TNO ICT, Delft.
4. Florian Kohlmayer et al. *Ambient Network Security Architecture*, Document IST–2002-507134-AN/WP7/D02, Deliverable 7.2 van het WWI Ambient Networks project, 8 februari 2006.
5. Punie, Y., Delaitre, S., Maghiros, I. & Wright, D (2005). *Dark scenarios on ambient intelligence: Highlighting risks and vulnerabilities* SWAMI Deliverable D2. Een rapport van het SWAMI consortium van de Europese Commissie, http://swami.jrc.es.
6. Friedewald, M., R. Lindner & D. Wright (2006). *Policy Options to Counteract Threats and Vulnerabilities in Ambient Intelligence*, SWAMI Deliverable D3. Een rapport van het SWAMI consortium van de Europese Commissie, http://swami.jrc.es.
7. Connecting Ambient Networks – Requirements and Concepts, D3.1, version 1.0, 28 June 2004, http://www.ambient-networks.org/index.html.
8. Book of Visions, 2001, WWRF.http://www.wireless-world-research.org/general_information/book_of_visions.php.
9. Van der Luit, R. (2006). *Herijking ICT veiligheidsbeleid*, DGET, concept, 14 juni 2006.